

DATA RECORDING/REPRODUCING METHOD AND DEVICE

Publication number: JP2001176191 (A)

Publication date: 2001-06-29

Inventor(s): CHIAKI SUSUMU

Applicant(s): SONY CORP

Classification:

- **international:** H04N5/85; G11B20/10; G11B20/12; H04N5/91; H04N5/92; H04N5/84; G11B20/10; G11B20/12; H04N5/91; H04N5/92; (IPC1-7): G11B20/10; H04N5/85

- **European:**

Application number: JP19990359398 19991217

Priority number(s): JP19990359398 19991217

Abstract of JP 2001176191 (A)

PROBLEM TO BE SOLVED: To make difficult the decoding and the disk copy of the data recorded on a disk like recording medium. **SOLUTION:** A data recording/reproducing device 10 is provided with a data processing means having at least an encode part 19 coding the data to be recorded on the disk like recording medium 30 and decoding the data to be reproduced recorded on the disk like recording medium 30. The encode part 19 records a disk ID peculiar to the disk like recording medium 30 during a frame synchronizing signal in the control area of the disk like recording medium 30 when the disk like recording medium 30 is initialized, and encodes the user data with the disk ID when the user data are recorded on the disk like recording medium 30.

inventor

— Date of application

Priority date

Priority

Document type

Language

Country

Category

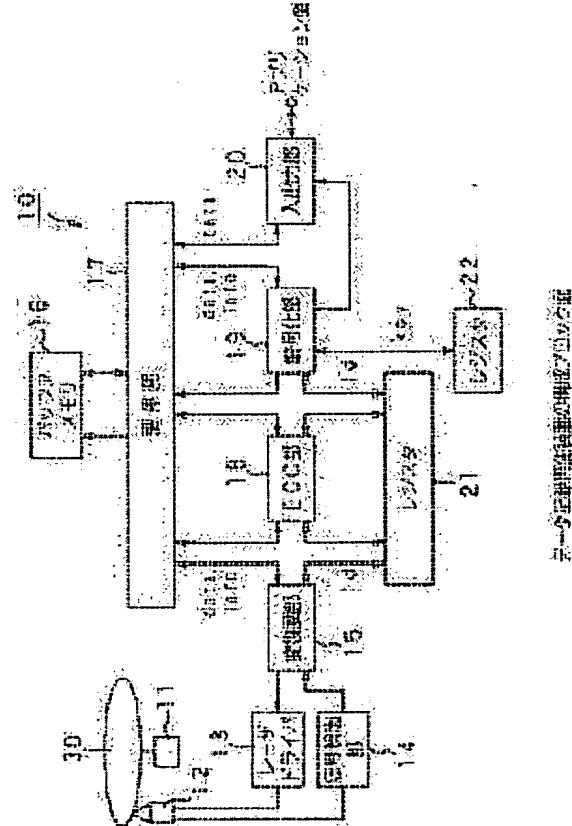
Classification

IPC

Publication date

Priority date

Priority



Data supplied from the esp@cenet database — Worldwide

【特許請求の範囲】

【請求項1】 ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、

上記ディスク状記録媒体の初期化時に、上記ディスク状記録媒体に固有の記録媒体識別情報を上記ディスク状記録媒体のコントロール領域における所定領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報を用いて上記ユーザデータを暗号化することを特徴とするデータ記録再生方法。

【請求項2】 上記所定領域は、データを記録するためのデータ記録領域以外の領域であることを特徴とする請求項1記載のデータ記録再生方法。

【請求項3】 上記所定領域は、フレーム同期信号を記録するためのフレーム同期信号記録領域であることを特徴とする請求項2記載のデータ記録再生方法。

【請求項4】 上記ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を、上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記記録媒体識別情報と上記記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項5】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、ユーザ領域における上記付加情報記録領域に記録し、

上記記録媒体鍵情報と上記ブロック情報を用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項4記載のデータ記録再生方法。

【請求項6】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック情報を取り出し

て、上記記録媒体鍵情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項5記載のデータ記録再生方法。

【請求項7】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、

上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項4記載のデータ記録再生方法。

【請求項8】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項7記載のデータ記録再生方法。

【請求項9】 上記ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を、上記記録媒体情報をとして上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項10】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を用いてブロック鍵情報を生成し、

上記ブロック鍵情報を、上記ブロック情報をとして上記ユーザ領域における上記付加情報記録領域に記録し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項9記載のデータ記録再生方法。

【請求項11】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項10記載のデータ記録再生方法。

【請求項12】 上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記記録媒体識別情報を用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、

上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記記録媒体情報を記録媒体鍵情報とし、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項13】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記記録媒体鍵情報と上記ブロック識別情報とを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、

上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、

上記ブロック情報をブロック鍵情報とし、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項12記載のデータ記録再生方法。

【請求項14】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック情報を取り出して、上記記録媒体鍵情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項13記載のデータ記録再生方法。

【請求項15】 上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、

上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、

上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項16】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報を上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、
上記ランダムデータを分割し、
上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、
上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、
上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報を上記記録媒体鍵情報を用いてブロック鍵情報を生成し、
上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項15記載のデータ記録再生方法。

【請求項17】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、
上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記記録媒体鍵情報を生成し、
上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ブロック識別情報と上記ブロック情報を上記記録媒体鍵情報を用いて上記ブロック鍵情報を生成し、
上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項16記載のデータ記録再生方法。

【請求項18】 上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを物理ブロック番号を用いて暗号化して、上記ディスク状記録媒体における各ブロック毎に固有の上記記録媒体識別情報を生成し、
上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、

上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1

記載のデータ記録再生方法。

【請求項19】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記物理ブロック番号を用いて暗号化して、上記各ブロック毎に固有のブロック識別情報を生成し、

上記ブロック識別情報を上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ランダムデータを分割し、

上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、

上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、

上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報を上記記録媒体鍵情報を用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項18記載のデータ記録再生方法。

【請求項20】 上記ディスク状記録媒体に記録されているユーザデータの再生時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ブロック識別情報と上記ブロック情報を上記記録媒体鍵情報を用いて上記ブロック鍵情報を生成し、

上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項19記載のデータ記録再生方法。

【請求項21】 上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報を若しくは上記ブロック情報が暗号化されていることを示していた場合には、

復号化して出力すべき旨のコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、

復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項6記載のデータ記録再生方法。

【請求項22】 上記ディスク状記録媒体に記録されて

いる制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、

復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、

復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項21記載のデータ記録再生方法。

【請求項23】 上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、

復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、

復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項8記載のデータ記録再生方法。

【請求項24】 上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、

復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、

復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項23記載のデータ記録再生方法。

【請求項25】 上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを上記記録媒体識別情報とし、この記録媒体識別情報を上記コントロール領域における上記所定領域としての付加情報を記録するための付加情報記録領域に記録し、

上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を上記コントロール領域における上記付加情報記録領域に記録し、

上記記録媒体識別情報と上記記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項26】 上記ディスク状記録媒体の初期化時に、

ランダムデータを発生し、このランダムデータを上記記録媒体識別情報とし、

上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を用いて記録媒体鍵情報を生成し、

上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データとともに、上記記録媒体識別情報と上記記録媒体情報を、上記記録媒体識別情報を上記コントロール領域における上記所定領域としてのデータ記録領域に記録することを特徴とする請求項1記載のデータ記録再生方法。

【請求項27】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、このブロック識別情報をユーザ領域における付加情報を記録するための付加情報記録領域に記録し、

30 上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、

上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いてブロック鍵情報を生成し、

上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項25記載のデータ記録再生方法。

【請求項28】 上記ディスク状記録媒体に対するユーザデータの記録時に、

上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記記録媒体鍵情報を生成し、

ランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、

上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時

情報の全部又は一部の情報であるブロック情報を用いてブロック鍵情報を生成し、上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータとともに、上記ブロック識別情報と上記ブロック情報を上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項26記載のデータ記録再生方法。

【請求項29】 上記ディスク状記録媒体の初期化における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を予め記憶していることを特徴とする請求項1記載のデータ記録再生方法。

【請求項30】 ディスク状記録媒体に対するブロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、

上記ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、上記ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、上記暗号化手段は、

上記ディスク状記録媒体の初期化時に、上記ディスク状記録媒体に固有の記録媒体識別情報を上記ディスク状記録媒体のコントロール領域における所定領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報を用いて上記ユーザデータを暗号化することを特徴とするデータ記録再生装置。

【請求項31】 上記所定領域は、データを記録するためのデータ記録領域以外の領域であることを特徴とする請求項30記載のデータ記録再生装置。

【請求項32】 上記所定領域は、フレーム同期信号を記録するためのフレーム同期信号記録領域であることを特徴とする請求項31記載のデータ記録再生装置。

【請求項33】 上記暗号化手段は、ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を、上記コントロール領域における付加情報を記録するための付加情報

記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体識別情報と上記記録媒体情報を用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項30記載のデータ記録再生装置。

【請求項34】 上記暗号化手段は、鍵情報を生成するユーザ領域用鍵情報生成手段と、暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報を用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項33記載のデータ記録再生装置。

【請求項35】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項34記載のデータ記録再生装置。

【請求項36】 上記暗号化手段は、ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生

し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項33記載のデータ記録再生装置。

【請求項37】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項36記載のデータ記録再生装置。

【請求項38】 上記暗号化手段は、
ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、
鍵情報を生成するコントロール領域用鍵情報生成手段と、
暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段と有し、
上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記コントロール領域用鍵情報生成手段によって、上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を用いて記録媒体鍵情報を生成し、上記記録媒体鍵情報を、上記記録媒体情報をとして上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを

特徴とする請求項30記載のデータ記録再生装置。

【請求項39】 上記暗号化手段は、
ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、
鍵情報を生成するユーザ領域用鍵情報生成手段と、
暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段と有し、
上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ユーザ領域用鍵情報生成手段によって、上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を用いてブロック鍵情報を生成し、上記ブロック鍵情報を、上記ブロック情報をとして上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項38記載のデータ記録再生装置。

【請求項40】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項39記載のデータ記録再生装置。

【請求項41】 上記暗号化手段は、
ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、
鍵情報を生成するコントロール領域用鍵情報生成手段と、
暗号化及び／又は復号化を行う第1及び第2のコントロール領域用暗号化及び／又は復号化手段と有し、
上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報

として上記コントロール領域における上記所定領域に記録し、上記第1のコントロール領域用暗号化及び／又は復号化手段によって、上記記録媒体識別情報を用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体情報を記録媒体鍵情報とし、上記第2のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項30記載のデータ記録再生装置。

【請求項42】 上記暗号化手段は、
ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、
鍵情報を生成するユーザ領域用鍵情報生成手段と、
暗号化及び／又は復号化を行う第1及び第2のユーザ領域用暗号化及び／又は復号化手段とを有し、
上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記第1のユーザ領域用暗号化及び／又は復号化手段によって、上記記録媒体鍵情報と上記ブロック識別情報とを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ブロック情報をブロック鍵情報とし、上記第2のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項41記載のデータ記録再生装置。

【請求項43】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック情報を用いて上記ブロック鍵情報を生成し、上記第2のユーザ領域用暗号化及び／

／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項42記載のデータ記録再生装置。
【請求項44】 上記暗号化手段は、
ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、
鍵情報を分割するコントロール領域用鍵情報分割手段と、
鍵情報を生成するコントロール領域用鍵情報生成手段と、
暗号化及び／又は復号化を行う第1及び第2のコントロール領域用暗号化及び／又は復号化手段とを有し、
上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記記録媒体識別情報として上記コントロール領域における上記所定領域に記録し、上記コントロール領域用鍵情報分割手段により上記ランダムデータを分割し、上記第1のコントロール領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報を用いて記録媒体鍵情報を生成し、上記第2のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項30記載のデータ記録再生装置。

【請求項45】 上記暗号化手段は、
ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、
鍵情報を分割するユーザ領域用鍵情報分割手段と、
鍵情報を生成するユーザ領域用鍵情報生成手段と、
暗号化及び／又は復号化を行う第1及び第2のユーザ領域用暗号化及び／又は復号化手段とを有し、
上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報として上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、上記ユーザ領域用鍵情報分割手段により上記ラン

ダムデータを分割し、上記第1のユーザ領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報を上記記録媒体鍵情報とを用いてブロック鍵情報を生成し、上記第2のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項4記載のデータ記録再生装置。

【請求項46】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報とを再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記ブロック識別情報と上記ブロック情報を生成し、上記第2のユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項4記載のデータ記録再生装置。

【請求項47】 上記暗号化手段は、ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、鍵情報を分割するコントロール領域用鍵情報分割手段と、鍵情報を生成するコントロール領域用鍵情報生成手段と、暗号化及び／又は復号化を行う第1、第2及び第3のコントロール領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生し、上記第1のコントロール領域用暗号化及び／又は復号化手段によりこのランダムデータを物理ブロック番号を用いて暗号化して、上記ディスク状記録媒体における各ブロック毎に固有の上記記録媒体識別情報を生成し、上記コントロール領域用鍵情報分割手段により上記ランダムデータを分割し、上記第2のコントロール領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体の初期化時における上記

ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報を暗号化して、記録媒体情報を生成し、上記記録媒体情報を上記コントロール領域における付加情報を記録するための付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記記録媒体情報を用いて記録媒体鍵情報を生成し、上記第3のコントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項3記載のデータ記録再生装置。

【請求項48】 上記暗号化手段は、ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を分割するユーザ領域用鍵情報分割手段と、鍵情報を生成するユーザ領域用鍵情報生成手段と、暗号化及び／又は復号化を行う第1、第2及び第3のユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、上記第1のユーザ領域用暗号化及び／又は復号化手段によりこのランダムデータを上記物理ブロック番号を用いて暗号化して、上記各ブロック毎に固有のブロック識別情報を生成し、上記ブロック識別情報を上記ディスク状記録媒体のユーザ領域における上記所定領域に記録し、

上記ユーザ領域用鍵情報分割手段により上記ランダムデータを分割し、上記第2のユーザ領域用暗号化及び／又は復号化手段によって、上記ランダムデータを分割して得られた一方のランダムデータを用いて、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報を暗号化して、ブロック情報を生成し、上記ブロック情報を上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記ランダムデータを分割して得られた他方のランダムデータと上記ブロック情報を上記記録媒体鍵情報を用いてブロック鍵情報を生成し、上記第3のユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項4記載のデータ記録再生装置。

【請求項49】 上記暗号化手段は、上記ディスク状記録媒体に記録されているユーザデータの再生時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により

上記記録媒体鍵情報を生成し、上記ユーザ領域を再生して上記ブロック識別情報と上記ブロック情報を取り出して、上記ユーザ領域用鍵情報生成手段により上記ブロック識別情報と上記ブロック情報と上記記録媒体鍵情報を用いて上記ブロック鍵情報を生成し、上記第3のユーザ領域用暗号化及び／又は復号化手段により上記暗号化ユーザデータを上記ブロック鍵情報を用いて復号化し、得られた上記ユーザデータを出力することを特徴とする請求項4 8記載のデータ記録再生装置。

【請求項5 0】 上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項3 5記載のデータ記録再生装置。

【請求項5 1】 上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項5 0記載のデータ記録再生装置。

【請求項5 2】 上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていることを示していた場合には、復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力し、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力しないことを特徴とする請求項3 7記載のデータ記録再生装置。

【請求項5 3】 上記暗号化手段は、上記ディスク状記録媒体に記録されている制御データ又はユーザデータの再生時に、再生されたブロックからの上記記録媒体識別情報若しくは上記ブロック識別情報又は上記暗号化制御

データ若しくは上記暗号化ユーザデータ又は上記記録媒体情報若しくは上記ブロック情報が暗号化されていないことを示していた場合には、復号化して出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを出力せず、復号化しないで出力すべき旨のコマンドを受けた場合には、上記暗号化制御データ若しくは上記暗号化ユーザデータを復号化して出力することを特徴とする請求項5 2記載のデータ記録再生装置。

【請求項5 4】 上記データ処理手段は、上記データ処理を行うためにデータを一時記憶する一時記憶手段を有することを特徴とする請求項3 0記載のデータ記録再生装置。

【請求項5 5】 上記データ処理手段は、上記ディスク状記録媒体に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ手段から出力された信号を電流－電圧変換して得られた信号からデータを検出する信号検出手段を有することを特徴とする請求項5 4記載のデータ記録再生装置。

【請求項5 6】 上記データ処理手段は、データの変調及び／又は復調を行う変復調手段と、データに対する誤り訂正及び／又は誤り検出手段と、外部とのデータの入出力を行うための入出力手段と、データに対する暗号化及び復号化に必要となる情報を保持する記憶手段と、上記変復調手段、上記誤り訂正及び／又は誤り検出手段、上記暗号化手段又は上記入出力手段と上記データ処理を行うためにデータを一時記憶する一時記憶手段との間で行われるデータの入出力を調停する調停手段とを少なくとも有することを特徴とする請求項3 0記載のデータ記録再生装置。

【請求項5 7】 上記暗号化手段は、ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、鍵情報を生成するコントロール領域用鍵情報生成手段と、

暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、上記ディスク状記録媒体の初期化時に、コントロール領域用ランダムデータ発生手段によりランダムデータを発生させ、このランダムデータを上記記録媒体識別情報とし、この記録媒体識別情報を上記コントロール領域における上記所定領域としての付加情報を記録するための付加情報記録領域に記録し、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を上記コントロール領域における上記付加情報記録領域に記録し、上記コントロール領域用鍵情報生成手段により上記記録媒体識別情報と上記記録媒体情報を用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を

を用いて制御データを暗号化し、得られた暗号化制御データを上記コントロール領域におけるデータ記録領域に記録することを特徴とする請求項54記載のデータ記録再生装置。

【請求項58】 上記暗号化手段は、
ランダムデータを発生させるコントロール領域用ランダムデータ発生手段と、
鍵情報を生成するコントロール領域用鍵情報生成手段と、
暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段とを有し、
上記ディスク状記録媒体の初期化時に、上記コントロール領域用ランダムデータ発生手段によりランダムデータを発生させ、このランダムデータを上記記録媒体識別情報とし、上記コントロール領域用鍵情報生成手段によって、上記記録媒体識別情報と、上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を用いて記録媒体鍵情報を生成し、上記コントロール領域用暗号化及び／又は復号化手段により上記記録媒体鍵情報を用いて制御データを暗号化し、得られた暗号化制御データとともに、上記記録媒体識別情報と上記記録媒体情報を、上記コントロール領域における上記所定領域としてのデータ記録領域に記録することを特徴とする請求項54記載のデータ記録再生装置。

【請求項59】 上記暗号化手段は、
ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、
鍵情報を生成するユーザ領域用鍵情報生成手段と、
暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、
上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、このブロック識別情報をユーザ領域における付加情報を記録するための付加情報記録領域に記録し、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を、上記ユーザ領域における上記付加情報記録領域に記録し、上記ユーザ領域用鍵情報生成手段により上記記録媒体鍵情報と上記ブロック識別情報と上記ブロック情報を用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータを上記ユーザ領域における上記データ記録領域に記録することを特

徴とする請求項57記載のデータ記録再生装置。

【請求項60】 上記暗号化手段は、
ランダムデータを発生させるユーザ領域用ランダムデータ発生手段と、

鍵情報を生成するユーザ領域用鍵情報生成手段と、
暗号化及び／又は復号化を行うユーザ領域用暗号化及び／又は復号化手段とを有し、

上記ディスク状記録媒体に対するユーザデータの記録時に、上記記録媒体識別情報と上記記録媒体情報を再生して取り出して、上記コントロール領域用鍵情報生成手段により上記記録媒体鍵情報を生成し、上記ユーザ領域用ランダムデータ発生手段によりランダムデータを発生し、このランダムデータを上記ディスク状記録媒体におけるブロックに固有のブロック識別情報とし、上記ユーザ領域用鍵情報生成手段によって、上記記録媒体鍵情報と、上記ブロック識別情報と、上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を用いてブロック鍵情報を生成し、上記ユーザ領域用暗号化及び／又は復号化手段により上記ブロック鍵情報を用いて上記ユーザデータを暗号化し、得られた暗号化ユーザデータとともに、上記ブロック識別情報と上記ブロック情報を上記ユーザ領域における上記データ記録領域に記録することを特徴とする請求項58記載のデータ記録再生装置。

【請求項61】 上記暗号化手段は、情報を記憶する記憶手段を有し、

上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を上記記憶手段に予め記憶していることを特徴とする請求項30記載のデータ記録再生装置。

【請求項62】 上記ディスク状記録媒体の初期化時における上記ディスク状記録媒体に関する情報である初期化時情報の全部又は一部の情報である記録媒体情報を及び／又は上記ディスク状記録媒体に対するユーザデータの記録時における上記ディスク状記録媒体に関する情報である記録時情報の全部又は一部の情報であるブロック情報を上記一時記憶手段に予め記憶していることを特徴とする請求項54記載のデータ記録再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ディスク状記録媒体に対するデータの記録及び／又は再生を行うデータ記録再生方法及びデータ記録再生装置に関する。

【0002】

【従来の技術】 例えば高画質のデジタルビデオ信号等

のディジタルデータを光学的に記録したディスク状記録媒体として、再生専用であるDVD (Digital Versatile Disc又は Digital Video Disc) が広く知られている。また最近では、このDVDフォーマットを用いて、追記や書き換えを可能としたディスク状記録媒体として、DVD-R (DVD-Recordable)、DVD-RW (DVD-ReWritable)、DVD-RAM (DVD-Random Access Memory) の商品化や開発が進められている。

【0003】このようなディスク状記録媒体においては、ユーザデータ、制御情報及びID情報等が1つのブロックとして誤り訂正符号化され、この誤り訂正符号化されたデータが変調され、さらに同期信号が付加されて記録される。

【0004】例えばDVDのフォーマットは、図16に示すように、ユーザデータ、制御情報及びID情報等からなる172バイト×192バイト=33024バイトのECC (Error Correcting Code) ブロックに対して同図中斜線部に示すパリティが付加されたいわゆる積符号の構成となる。DVDにおいては、誤り訂正符号としてRS (Read Solomon Code) が用いられる。DVDにおいては、行方向をC1、列方向をC2とすると、C1は、RS (182, 172, 11)、C2は、RS (208, 192, 17) である。

【0005】この1ブロック分のデータは、ディスク状記録媒体上の16セクタ分に相当する。ディスク状記録媒体の1セクタは、26フレームから構成され、1フレームは、91バイトのデータから構成される。また、各フレームには、フレーム同期信号が付加される。すなわち、ディスク状記録媒体上に並べられるパリティ以外のデータは、図17に示すように、91バイト×416フレーム (16セクタ×26フレーム) から構成される。

【0006】ディスク状記録媒体においては、データの再生時には、フレーム同期信号 (Frame Sync; 以下、FSと記す。) により同期をとった後、ID情報によりセクタ同期をとることによって、1ブロック上のデータの位置が判別できることから、ID情報は、ディスク状記録媒体上でデータ方向に配置されている必要がある。また、ID情報は、各物理セクタ内で同じ位置に配置されている必要がある。そのため、ディスク状記録媒体上に並べられるパリティ以外のデータにおいては、例えばDVDの場合には同図に示すように、FSを記録するためのFS領域が各物理セクタの先頭に位置している。

【0007】このようなディスク状記録媒体に対するディジタルデータの記録及び/又は再生を行うデータ記録再生装置は、例えば図18に示すような各部を備える。すなわち、データ記録再生装置100は、ディスク状記録媒体150を回転駆動するスピンドルモータ101と、ディスク状記録媒体150に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ102と、この光学ピックアップ102におけるレーザダ

イオードを駆動するレーザドライバ103と、光学ピックアップ102から出力された信号を電流-電圧変換 (IV変換) して得られたRF (Radio Frequency) 信号からデータを検出する信号検出部104と、後述するバッファメモリ106から読み出したデータを変調するとともに、信号検出部104から供給されるデータを復調する変復調部105と、データに各種処理を施すためにデータを一時記憶するバッファメモリ106と、このバッファメモリ106と、変復調部105、後述するECC部108又は後述する入出力部109との間で行われるデータの入出力を調停する調停部107と、データに対する誤り訂正及び/又は誤り検出を行うECC部108と、外部とのデータの入出力を行うためのインターフェースである入出力部109とを備える。

【0008】スピンドルモータ101は、図示しないサーボ回路の制御の下に、ディスク状記録媒体150を所定の回転速度により回転駆動する。

【0009】光学ピックアップ102は、ディスク状記録媒体150に対するデータの記録時には、後段のレーザドライバ103により駆動された図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体150上に照射し、記録すべきデータをビット列としてディスク状記録媒体150に記録する。

【0010】また、光学ピックアップ102は、ディスク状記録媒体150に記録されているデータの再生時には、図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体150上に照射するとともに、ディスク状記録媒体150の表面で反射回折された戻り光を図示しないフォトダイオードにより受光して電気信号に変換することによって、ディスク状記録媒体150に記録されているデータを読み出す。

【0011】このような光学ピックアップ102は、ディスク状記録媒体150に対してデータを記録時及び再生時には、受光した戻り光に基づいて、トラッキング制御やフォーカス制御がされ、ディスク状記録媒体150に対してアクセスする。

【0012】レーザドライバ103は、変復調部105から供給されるデータに基づいて、光学ピックアップ102におけるレーザダイオードを駆動する。

【0013】信号検出部104は、光学ピックアップ102から出力された信号を電流-電圧変換して得られたRF信号からクロックを再生し、このクロックを基準としてRF信号を順次処理することによって、データを検出する。信号検出部104は、検出したデータを変復調部105に供給する。

【0014】変復調部105は、ディスク状記録媒体150に対するデータの記録時には、調停部107を介してバッファメモリ106からECCブロック単位で記録

すべきデータを読み出し、これらのデータを所定のフォーマットにより変調する。変復調部105は、同期信号やその他の情報をデータに付加し、変調して得られたデータをレーザドライバ103に供給する。

【0015】また、変復調部105は、ディスク状記録媒体150に記録されているデータの再生時には、信号検出部104から供給されるデータに対して、FSによるフレーム同期及びブロックアドレスによるブロック同期をとり、これらのフレーム同期及びブロック同期のタイミングを基準にして順次供給されるデータを復調し、調停部107を介してバッファメモリ106に供給する。

【0016】バッファメモリ106は、ディスク状記録媒体150に対するデータの記録時には、入出力部109により外部のアプリケーション側から入力されたデータが調停部107を介して供給され、このデータを一時記憶する。バッファメモリ106により一時記憶されたデータは、調停部107を介してECC部108により読み出される。そして、バッファメモリ106は、ECC部108により誤り訂正符号化されたデータが調停部107を介して供給され、このデータを一時記憶する。バッファメモリ106により一時記憶されたデータは、調停部107を介して変復調部105により所定順序で読み出される。

【0017】また、バッファメモリ106は、ディスク状記録媒体150に記録されているデータの再生時には、変復調部105により復調されたデータが調停部107を介して供給され、このデータを一時記憶する。バッファメモリ106により一時記憶されたデータは、調停部107を介してECC部108により読み出される。そして、バッファメモリ106は、ECC部108により誤り検出処理されたデータが調停部107を介して供給され、このデータを一時記憶する。バッファメモリ106により一時記憶されたデータは、調停部107を介して入出力部109により所定順次で読み出される。

【0018】調停部107は、変復調部105、ECC部108又は入出力部109のそれぞれに対してバッファメモリ106を使用する占有権を割り当てる、バッファメモリ106と、変復調部105、ECC部108又は入出力部109との間で行われるデータの入出力を調停する。

【0019】ECC部108は、ディスク状記録媒体150に対するデータの記録時には、入出力部109により外部のアプリケーション側から入力されてバッファメモリ106により一時記憶されたデータを調停部107を介して読み出し、このデータを誤り訂正符号化する。ECC部108は、誤り訂正符号化したデータを調停部107を介してバッファメモリ106に供給する。

【0020】また、ECC部108は、ディスク状記録

媒体150に記録されているデータの再生時には、変復調部105により復調されてバッファメモリ106により一時記憶されたデータを調停部107を介して読み出し、このデータの誤り検出を行う。ECC部108は、誤り検出を行ったデータを調停部107を介してバッファメモリ106に供給する。

【0021】入出力部109は、ディスク状記録媒体150に対するデータの記録時には、外部のアプリケーション側から入力されたデータを調停部107を介してバッファメモリ106に供給する。

【0022】また、入出力部109は、ディスク状記録媒体150に記録されているデータの再生時には、ECC部108により誤り検出が行われてバッファメモリ106に一時記憶されているデータを調停部107を介して読み出し、外部のアプリケーション側へと出力する。

【0023】このようなデータ記録再生装置100は、ディスク状記録媒体150に対するデータの記録時には、ディスク状記録媒体150に予め形成されているブリピットによる物理アドレスを光学ピックアップ102を介して読み出し、変復調部105により検出する。データ記録再生装置100は、この物理アドレスのタイミングを基準にしてディスク状記録媒体150に対してECCブロック単位で順次記録する。

【0024】また、データ記録再生装置100は、ディスク状記録媒体150に記録されているデータの再生時には、変復調部105により物理アドレスを検出し、そのタイミングを基準にしてディスク状記録媒体150からECCブロック単位で順次再生する。

【0025】【発明が解決しようとする課題】ところで、上述したようなディスク状記録媒体において、当該ディスク状記録媒体に記録されているデータの解読や当該ディスク状記録媒体自体の複製、すなわち、ディスクコピー等に対する措置が考慮されていない方式やフォーマットにより構成されているものは、いかなるデータ記録再生装置であっても記録及び／又は再生され得る。

【0026】このような現状に鑑みて、近年では、このようなディスク状記録媒体に記録されているデータの解読やディスクコピー等に対する措置が考えられている。

【0027】例えば、ディスク状記録媒体から正当なデータ記録再生装置のみがデータを再生できるようにするため、上述したECC部や変復調部等のデータ処理部と外部のアプリケーション側との間に暗号化部を備えるデータ記録再生装置がある。

【0028】このデータ記録再生装置は、ディスク状記録媒体の初期化時に、ランダムデータを発生し、このランダムデータをディスク状記録媒体に固有のディスクIDとして、ディスク状記録媒体のコントロール領域のデータ中に記録する。そして、このデータ記録再生装置は、ユーザデータの記録時には、ディスクIDを用いて

ユーザデータを暗号化してディスク状記録媒体に記録し、ユーザデータの再生時には、再生したデータをディスクIDを用いて復号化する。

【0029】このようにすることによって、暗号化部を備えないデータ記録再生装置は、ディスク状記録媒体から再生したデータを復号化することができない。また、このような方法をとることによって、ディスク状記録媒体のユーザ領域のデータの再生時に復号化せず、又は、暗号化部を通さずに、このデータを、他のディスク状記録媒体に暗号化することなく、又は、暗号化部を通さずに記録した場合でも、ディスクIDが異なることから、復号化することができない。

【0030】しかしながら、このような方法では、初期化したディスク状記録媒体に暗号化したデータを記録し、この暗号化されたデータを復号化せず、又は、暗号化部を通さずに再生するといった手順を繰り返すことによって、不当な第三者は、ディスクIDを知ることができます。そのため、不当な第三者は、ディスクIDを知ることによって、上述したECC部や変復調部等のデータ処理部からの出力に対して復号化できるようになってしまっていった問題があった。

【0031】また、暗号化部を備えるデータ記録再生装置であっても、ファームウェア等を改変したものでは、再生したデータを復号化できてしまうことが考えられる。ディスクIDがわかれば、暗号化部を備えない不当なデータ記録再生装置であっても、そのディスクIDを用いて暗号化したデータを生成し、他のディスク状記録媒体に記録することができてしまう。

【0032】さらに、ディスク状記録媒体のコントロール領域を含む全ての領域のデータを再生する際に、データの復号化を行わず、又は、暗号化部を通さずに、このデータを、他のディスク状記録媒体に暗号化することなく、又は、暗号化部を通さずに記録した場合には、ディスクIDも他のディスク状記録媒体にコピーされることとなり、不当なデータ記録再生装置であっても、データを復号化することができてしまう。

【0033】本発明は、このような実情に鑑みてなされたものであり、ディスク状記録媒体に対する従来の記録及び／又は再生の方式における問題を解決し、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とするデータ記録再生方法及びデータ記録再生装置を提供することを目的とするものである。

【0034】

【課題を解決するための手段】上述した目的を達成する本発明にかかるデータ記録再生方法は、ディスク状記録媒体に対するプロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対す

るユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化することを特徴としている。

【0035】このような本発明にかかるデータ記録再生方法は、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化する。

【0036】また、上述した目的を達成する本発明にかかるデータ記録再生装置は、ディスク状記録媒体に対するプロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、暗号化手段は、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化することを特徴としている。

【0037】このような本発明にかかるデータ記録再生装置は、暗号化手段によって、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化する。

【0038】

【発明の実施の形態】以下、本発明を適用した具体的な実施の形態について図面を参照しながら詳細に説明する。

30 【0039】本発明を適用した実施の形態は、いわゆる光ディスクのようなディスク状記録媒体に対するデータの記録及び／又は再生を行うデータ記録再生装置である。

【0040】実施の形態として示すデータ記録再生装置に適用されるディスク状記録媒体におけるフォーマットは、図1に示すように、フレーム同期信号(Frame Sync; 以下、FSと記す。)を記録するためのフレーム同期信号記録領域であるFS領域と、例えばアドレス情報等のデータ以外の付加情報であるIDSを記録するための付加情報記録領域であるIDS領域と、データであるUDSを記録するためのデータ記録領域であるUDS領域とにより1プロックのデータが構成されるものである。UDS領域の情報ワードは、データ記録再生装置に対する外部のアプリケーション側との間で入出力される通常のデータ部であり、IDS領域の情報ワードは、データ記録再生装置に対する外部のアプリケーション側との間でそのままの形式では入出力されないものである。なお、ディスク状記録媒体においては、このように、UDS領域とIDS領域とに対して、それぞれ、データの入出力等の制御が可能であれば、必ずしも符号プロック

として区別しなくてもよい。

【0041】この1ブロックのデータは、同図中斜線部に示すように、例えばRS(Read Solomon Code)により誤り訂正符号化される。例えば、同図に示すように、UDSは、RS(248, 216, 33)×304符号により構成され、符号の情報ワードは、304バイト×216バイト=65664バイト≈約64Kバイトである。また、例えば、同図に示すように、IDSは、RS(62, 30, 33)×24符号により構成され、符号の情報ワードは、24バイト×30バイト=720バイトである。

【0042】さらに、ディスク状記録媒体には、当該ディスク状記録媒体に固有の記録媒体識別情報であるディスクID(disk_id)やブロックに固有のブロック識別情報であるブロックID(block_id)といったデータを暗号化する際に用いる暗号鍵のID情報が誤り訂正符号化されて例えばFS領域といった秘匿性のある情報中に記録される。このID情報は、例えば、RS(62, 216, 33)×1符号により構成され、符号の情報ワードは、1バイト×30バイト=30バイトである。

【0043】ディスク状記録媒体においては、一般に、UDSは、数百バイト乃至数十Kバイトで構成され、IDSは、数十バイト乃至数百バイトで構成され、ID情報は、数十バイトで構成される。

【0044】この1ブロック分のデータは、496フレームから構成され、1フレームは、155バイトのデータから構成される。また、各フレームには、FSが付加される。すなわち、ディスク状記録媒体上に並べられるパリティ以外のデータは、図2に示すように、155バイト×496フレームから構成される。

【0045】なお、先に図1に示したUDS及びIDSの情報は、フレーム内のデータであり、ID情報は、1ビットずつFS領域に記録されるものである。

【0046】このようなディスク状記録媒体に対するデジタルデータの記録及び/又は再生を行うデータ記録再生装置は、図3に示すような各部を備える。すなわち、データ記録再生装置10は、ディスク状記録媒体30を回転駆動するスピンドルモータ11と、ディスク状記録媒体30に対してレーザ光を照射するとともにその戻り光を受光する光学ピックアップ手段である光学ピックアップ12と、この光学ピックアップ12におけるレーザダイオードを駆動するレーザドライバ13と、光学ピックアップ12から出力された信号を電流-電圧変換(IV変換)して得られたRF(Radio Frequency)信号からデータを検出する信号検出手段である信号検出部14と、後述するバッファメモリ16から読み出したデータを変調するとともに、信号検出部14から供給されるデータを復調する変復調手段である変復調部15と、データに各種処理を施すためにデータを一時記憶する一時記憶手段であるバッファメモリ16と、このバッファ

メモリ16と、変復調部15、後述するECC部18、後述する暗号化部19又は後述する入出力部20との間で行われるデータの入出力を調停する調停手段である調停部17と、データに対する誤り訂正及び/又は誤り検出を行う誤り訂正及び/又は誤り検出手段であるECC部18と、バッファメモリ16から読み出した記録すべきデータを暗号化するとともに、バッファメモリ16から読み出した再生すべきデータを復号化する暗号化手段である暗号化部19と、外部とのデータの入出力をを行うためのインターフェースとなる入出力手段である入出力部20と、データに対する暗号化及び復号化に必要となる後述する各種情報を保持する記憶手段であるレジスタ21, 22とを備える。

【0047】スピンドルモータ11は、図示しないサーボ回路の制御の下に、ディスク状記録媒体30を所定の回転速度により回転駆動する。

【0048】光学ピックアップ12は、ディスク状記録媒体30に対するデータの記録時には、後段のレーザドライバ13により駆動された図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体30上に照射し、記録すべきデータをビット列としてディスク状記録媒体30に記録する。

【0049】また、光学ピックアップ12は、ディスク状記録媒体30に記録されているデータの再生時には、図示しないレーザダイオードからのレーザ光を図示しない対物レンズにより集光してディスク状記録媒体30上に照射するとともに、ディスク状記録媒体30の表面で反射回折された戻り光を図示しないフォトダイオードにより受光して電気信号に変換することによって、ディスク状記録媒体30に記録されているデータを読み出す。

【0050】このような光学ピックアップ12は、ディスク状記録媒体30に対してデータを記録時及び再生時には、受光した戻り光に基づいて、トラッキング制御やフォーカス制御がされ、ディスク状記録媒体30に対してアクセスする。

【0051】レーザドライバ13は、変復調部15から供給されるデータに基づいて、光学ピックアップ12におけるレーザダイオードを駆動する。

【0052】信号検出部14は、光学ピックアップ12から出力された信号を電流-電圧変換して得られたRF信号からクロックを再生し、このクロックを基準としてRF信号を順次処理することによって、データを検出する。信号検出部14は、検出したデータを変復調部15に供給する。

【0053】変復調部15は、ディスク状記録媒体30に対するデータの記録時には、調停部17を介してバッファメモリ16からブロック単位で記録すべきデータを読み出し、これらのデータを所定のフォーマットにより変調する。変復調部15は、同期信号やバッファメモリ

16から調停部17を介して読み出したその他の情報をデータに付加し、変調して得られたデータをレーザドライバ13に供給する。この際、変復調部15は、暗号化部19により生成されてレジスタ21に保持されている上述したID情報を読み出す。このID情報は、レーザドライバ13に供給するデータに付加される。

【0054】また、変復調部15は、ディスク状記録媒体30に記録されているデータの再生時には、信号検出部14から供給されるデータに対して、FSによるフレーム同期及びブロックアドレスによるブロック同期をとり、これらのフレーム同期及びブロック同期のタイミングを基準にして順次供給されるデータを復調し、得られたデータやその他の情報を調停部17を介してバッファメモリ16に供給する。

【0055】バッファメモリ16は、ディスク状記録媒体30に対するデータの記録時には、入出力部20により外部のアプリケーション側から入力されたデータが調停部17を介して供給され、このデータを一時記憶する。バッファメモリ16により一時記憶されたデータは、調停部17を介して暗号化部19により読み出される。そして、バッファメモリ16は、暗号化部19により暗号化されたデータが調停部17を介して供給され、このデータを一時記憶する。バッファメモリ16により一時記憶されたデータは、調停部17を介してECC部18により読み出される。そして、バッファメモリ16は、ECC部18により誤り訂正符号化されたデータが調停部17を介して供給され、このデータを一時記憶する。バッファメモリ16により一時記憶されたデータは、調停部17を介して変復調部15により所定順序で読み出される。

【0056】また、バッファメモリ16は、ディスク状記録媒体30に記録されているデータの再生時には、変復調部15により復調されたデータが調停部17を介して供給され、このデータを一時記憶する。バッファメモリ16により一時記憶されたデータは、調停部17を介してECC部18により読み出される。そして、バッファメモリ16は、ECC部18により誤り検出処理されたデータが調停部17を介して供給され、このデータを一時記憶する。バッファメモリ16により一時記憶されたデータは、調停部17を介して入出力部20により所定順次で読み出される。

【0057】調停部17は、変復調部15、ECC部18、暗号化部19又は入出力部20のそれぞれに対してバッファメモリ16を使用する占有権を割り当て、バッファメモリ16と、変復調部15、ECC部18、暗号化部19又は入出力部20との間で行われるデータの入

出力を調停する。

【0058】ECC部18は、ディスク状記録媒体30に対するデータの記録時には、暗号化部19により暗号化されてバッファメモリ16により一時記憶されたデータを調停部17を介して読み出し、このデータを誤り訂正符号化する。ECC部18は、誤り訂正符号化したデータを調停部17を介してバッファメモリ16に供給する。

【0059】また、ECC部18は、ディスク状記録媒体30に記録されているデータの再生時には、変復調部15により復調されてバッファメモリ16により一時記憶されたデータを調停部17を介して読み出し、このデータの誤り検出を行う。ECC部18は、誤り検出を行ったデータを調停部17を介してバッファメモリ16に供給する。

【0060】暗号化部19は、例えば、上述したディスク状記録媒体30に固有のディスクID(disk_id)となるランダムデータの発生、データを暗号化する際に用いる鍵情報の生成・分割、データの暗号化・復号化といった処理に関わる演算を行う。

【0061】暗号化部19は、ディスク状記録媒体30に対するデータの記録時には、入出力部20により外部のアプリケーション側から入力されてバッファメモリ16により一時記憶されたデータを調停部17を介して読み出し、このデータを暗号化する。暗号化部19は、暗号化したデータを調停部17を介してバッファメモリ16に供給する。

【0062】また、暗号化部19は、ディスク状記録媒体30に記録されているデータの再生時には、ECC部18により誤り検出されてバッファメモリ16により一時記憶されたデータを調停部17を介して読み出し、このデータを復号化する。暗号化部19は、復号化したデータを調停部17を介してバッファメモリ16に供給する。

【0063】入出力部20は、ディスク状記録媒体30に対するデータの記録時には、外部のアプリケーション側から入力されたデータを調停部17を介してバッファメモリ16に供給する。

【0064】また、入出力部20は、ディスク状記録媒体30に記録されているデータの再生時には、暗号化部19により復号化されてバッファメモリ16に一時記憶されているデータを調停部17を介して読み出し、後述するように、暗号化部19の制御の下に、外部のアプリケーション側へと出力する。

【0065】レジスタ21は、暗号化部19により生成された上述したID情報を保持する。

【0066】レジスタ22は、暗号化部19により生成された暗号化の際に用いる鍵情報を保持する。

【0067】このようなデータ記録再生装置10は、上述したID情報が外部との間で入出力されることは好ま

しくないことから、これらの各部のうち、少なくとも、変復調部15、調停部17、ECC部18、暗号化部19、入出力部20及びレジスタ21、22がチップ化され、データ処理を行うデータ処理手段であるデータ処理部として構成される。このように暗号化部19をデータ処理部内に構成することによって、データ記録再生装置10は、図1及び図2に示したようなフォーマットのディスク状記録媒体30に対するデータの記録及び／又は再生を行うことができる。なお、同図において、dataは、後述するcont_data,control_data,user_data,blk_10 dataのうちのいずれか、すなわち、各種データを総称するものであり、infoは、後述するdisk_info,blk_infoのうちのいずれか、すなわち、各種情報を総称するものであり、idは、後述するdisk_id,blk_idのうちのいずれか、すなわち、ID情報を総称するものであり、keyは、後述するdisk_key,blk_keyのうちのいずれか、すなわち、鍵情報を総称するものである。

【0068】以下、データ記録再生装置10における基本的な動作について説明する。

【0069】まず、データ記録再生装置10がディスク状記録媒体30を初期化する場合について説明する。

【0070】データ記録再生装置10は、図4に示すように、ステップS1において、暗号化部19によりランダムデータを発生し、このランダムデータをディスク状記録媒体30に固有のディスクID(disk_id)とする。データ記録再生装置10は、このdisk_idをレジスタ21に供給して保持させる。

【0071】続いて、データ記録再生装置10は、ステップS2において、図示しないCPU(Central Processing Unit)及び図示しないインターフェースにより設定されてバッファメモリ16に保持されているディスク状記録媒体30に関する情報(disk_info)を調停部17を介して暗号化部19に供給し、暗号化部19によって、disk_idとdisk_infoとを用いてディスク状記録媒体30に記録するデータを暗号化するための鍵情報(disk_key)を生成する。データ記録再生装置10は、このdisk_keyをレジスタ22に供給して保持させる。

【0072】続いて、データ記録再生装置10は、ステップS3において、入出力部20により外部のアプリケーション側から入力されてバッファメモリ16に保持されている制御データ(control_data)、すなわち、ディスク状記録媒体30のコントロール領域に記録すべきデータを調停部17を介して暗号化部19に供給し、暗号化部19によって、control_dataをdisk_keyを用いて暗号化する。データ記録再生装置10は、この暗号化して得られた暗号化制御データ(cont_data)を調停部17を介してバッファメモリ16に供給して保持させる。なお、コントロール領域は、例えばディスク状記録媒体30の最内周側及び／又は最外周側に設けられる領域である。

【0073】続いて、データ記録再生装置10は、ステップS4において、ECC部18によって、レジスタ21に保持されているdisk_idと、バッファメモリ16に保持されているdisk_info,cont_dataとを読み出し、これらのdisk_id,disk_info,cont_dataに対して誤り訂正符号化を行う。データ記録再生装置10は、誤り訂正符号化したdisk_idをレジスタ21に供給して保持するとともに、誤り訂正符号化したdisk_info,cont_dataを調停部17を介してバッファメモリ16に供給して保持させる。

【0074】続いて、データ記録再生装置10は、ステップS5において、変復調部15によって、レジスタ21に保持されているdisk_idと、バッファメモリ16に保持されているdisk_info,cont_dataとを読み出し、disk_info,cont_dataを所定のフォーマットにより変調するとともに、disk_idをFS中に挿入する。

【0075】そして、データ記録再生装置10は、ステップS6において、ディスク状記録媒体30のフォーマットにしたがうブロック構成となったこれらのdisk_id,disk_info,cont_dataをレーザドライブ13に供給し、光学ピックアップ12によりブロック単位でディスク状記録媒体30のコントロール領域に記録する。なお、infoは、ディスク状記録媒体30における例えばIDSといった通常ユーザがアクセスできないデータ上に記録される。

【0076】このようにして、データ記録再生装置10は、ディスク状記録媒体30を初期化する。

【0077】つぎに、データ記録再生装置10がディスク状記録媒体30に対してユーザデータ(user_data)を記録する場合について説明する。

【0078】データ記録再生装置10は、ディスク状記録媒体30の初期化後に当該ディスク状記録媒体30を交換していない場合には、レジスタ22に保持されているdisk_keyを用いて記録すべきデータを暗号化する。

【0079】一方、データ記録再生装置10は、ディスク状記録媒体30の初期化後に当該ディスク状記録媒体30と異なるディスク状記録媒体に交換した場合には、レジスタ22に保持されているdisk_keyを用いることはできない。

【0080】そこでまず、データ記録再生装置10は、図5に示すように、ステップS11において、交換されて図示しない装着部に装着されたディスク状記録媒体30のコントロール領域中のブロックを再生する。

【0081】続いて、データ記録再生装置10は、ステップS12において、変復調部15によりディスク状記録媒体30から読み出したdisk_info,cont_dataを復調し、調停部17を介してバッファメモリ16に供給して保持させるとともに、変復調部15によりFS領域から抽出したdisk_idをレジスタ21に供給して保持させる。

【0082】続いて、データ記録再生装置10は、ステップS13において、ECC部18によって、レジスタ21からdisk_idを読み出すとともに、バッファメモリ16から調停部17を介してdisk_info,cont_dataを読み出し、これらのdisk_id,disk_info,cont_dataの誤り検出を行う。データ記録再生装置10は、誤り検出したdisk_idをレジスタ21に供給して保持させるとともに、誤り検出したdisk_info,cont_dataを調停部17を介してバッファメモリ16に供給して保持させる。

【0083】続いて、データ記録再生装置10は、ステップS14において、暗号化部19によって、レジスタ21からdisk_idを読み出すとともに、バッファメモリ16から調停部17を介してdisk_infoを読み出し、これらのdisk_idとdisk_infoとを用いてdisk_keyを生成する。データ記録再生装置10は、生成したdisk_keyをレジスタ22に供給して保持させる。

【0084】続いて、データ記録再生装置10は、ステップS15において、暗号化部19によりランダムデータを発生し、このランダムデータをディスク状記録媒体30のブロックに固有のブロックID(blk_id)とする。データ記録再生装置10は、このblk_idをレジスタ21に供給して保持させる。

【0085】続いて、データ記録再生装置10は、ステップS16において、図示しないCPU及び図示しないインターフェースにより設定されてバッファメモリ16に保持されているディスク状記録媒体30のブロックに関する情報(blk_info)を調停部17を介して暗号化部19に供給するとともに、disk_keyをレジスタ22から暗号化部19に供給し、暗号化部19によって、disk_keyとblk_infoと、さらに必要に応じてblk_idとを用いてディスク状記録媒体30のブロックに記録するデータを暗号化するための鍵情報(blk_key)を生成する。データ記録再生装置10は、このblk_keyをレジスタ22に供給して保持させる。

【0086】続いて、データ記録再生装置10は、ステップS17において、暗号化部19によって、入出力部20により外部のアプリケーション側から入力されてバッファメモリ16により一時記憶されたuser_dataを調停部17を介して読み出し、このuser_dataをblk_keyを用いて暗号化する。データ記録再生装置10は、この暗号化して得られた暗号化ユーザデータ(blk_data)を調停部17を介してバッファメモリ16に供給して保持させる。

【0087】続いて、データ記録再生装置10は、ステップS18において、ECC部18によって、バッファメモリ16に保持されているblk_info,blk_dataと、必要に応じてレジスタ21に保持されているblk_idとを読み出し、これらのblk_info,blk_data,blk_idに対して誤り訂正符号化を行う。データ記録再生装置10は、誤り訂正符号化したblk_info,blk_dataを調停部17を介し

てバッファメモリ16に供給して保持させるとともに、誤り訂正符号化したblk_idをレジスタ21に供給して保持させる。

【0088】続いて、データ記録再生装置10は、ステップS19において、変復調部15によって、バッファメモリ16に保持されているblk_info,blk_dataと、レジスタ21に保持されているblk_idとを読み出し、blk_info,blk_dataを所定のフォーマットにより変調するとともに、blk_idをFS中に挿入する。

【0089】そして、データ記録再生装置10は、ステップS20において、ディスク状記録媒体30のフォーマットにしたがうブロック構成となったこれらのblk_info,blk_data,blk_idをレーザドライブ13に供給し、光学ピックアップ12によりブロック単位でディスク状記録媒体30のユーザ領域に記録する。なお、infoは、ディスク状記録媒体30における例えばIDSといった通常ユーザがアクセスできないデータ上に記録される。

【0090】このようにして、データ記録再生装置10は、ディスク状記録媒体30に対してユーザデータを記録する。

【0091】つぎに、データ記録再生装置10がディスク状記録媒体30に記録されているユーザデータを再生する場合について説明する。

【0092】データ記録再生装置10は、ディスク状記録媒体30に対するユーザデータの記録時と同様に、レジスタ21にdisk_idを保持しているものとする。

【0093】そして、データ記録再生装置10は、図6に示すように、ステップS21において、ディスク状記録媒体30のユーザ領域の所望のブロックを再生する。

【0094】続いて、データ記録再生装置10は、ステップS22において、変復調部15によりディスク状記録媒体30から読み出したblk_info,blk_dataを復調し、調停部17を介してバッファメモリ16に供給して保持させる。また、データ記録再生装置10は、必要に応じて、変復調部15によりblk_idをFS領域から抽出し、抽出したblk_idをレジスタ21に供給して保持させる。

【0095】続いて、データ記録再生装置10は、ステップS23において、ECC部18によって、バッファメモリ16から調停部17を介してblk_info,blk_dataを読み出すとともに、必要に応じて、レジスタ21からblk_idを読み出し、これらのblk_info,blk_data,blk_idの誤り検出を行う。データ記録再生装置10は、誤り検出したblk_info,blk_dataを調停部17を介してバッファメモリ16に供給して保持せるとともに、blk_idをレジスタ21に供給して保持させる。

【0096】続いて、データ記録再生装置10は、ステップS24において、暗号化部19によって、バッファメモリ16から調停部17を介してblk_infoを読み出すとともに、必要に応じて、レジスタ21からblk_idを読

み出し、さらにレジスタ22からdisk_keyを読み出し、これらのblk_infoとdisk_keyと、さらに必要に応じてblk_idとを用いてblk_keyを生成する。データ記録再生装置10は、生成したblk_keyをレジスタ22に供給して保持させる。

【0097】続いて、データ記録再生装置10は、ステップS25において、暗号化部19によって、バッファメモリ16により一時記憶されたblk_dataを調停部17を介して読み出し、このblk_dataをblk_keyを用いて復号化する。データ記録再生装置10は、この復号化して得られたuser_dataを調停部17を介してバッファメモリ16に供給して保持させる。

【0098】そして、データ記録再生装置10は、ステップS26において、入出力部20によって、バッファメモリ16により一時記憶されたuser_dataを調停部17を介して読み出し、暗号化部19の制御の下に、外部のアプリケーション側へと出力する。

【0099】このようにして、データ記録再生装置10は、ディスク状記録媒体30に記録されているユーザデータを再生する。

【0100】なお、データ記録再生装置10においては、infoは、入出力部20を介して入出力をを行わず、図示しないCPUにより設定された必要な情報のみが図示しないインターフェースを介して入出力される。

【0101】以下、このようなデータ記録再生装置10における暗号化部19の具体的な動作について図7乃至図14を用いて説明する。

【0102】まず、データ記録再生装置10における第1の実施の形態について図7を用いて説明する。この第1の実施の形態は、データ記録再生装置10は、disk_idを用いてデータを暗号化するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおける例えば30バイト程度の任意のバイト数を有するFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、パリティは含まれていない。

【0103】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び/又は復号化を行うコントロール領域用暗号化及び/又は復号化手段である暗号化/復号化部e()及びユーザ領域用暗号化及び/又は復号化手段である暗号化/復号化部e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける

各部は、共通化されてもよく、例えば、鍵情報生成部f(), f'(), 暗号化/復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0104】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r()によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体30に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のFS領域に記録する。

【0105】また、暗号化部19は、初期化時におけるディスク状記録媒体30に関する各種情報（初期化時情報）であるinfo_dの全部又は一部の情報（記録媒体情報）を、図示しないCPUによりdisk_infoとして設定され、コントロール領域のブロック内のIDS領域に記録する。なお、初期化時におけるディスク状記録媒体30に関する各種情報とは、例えば、ディスク状記録媒体30の利用者情報やパスワード、ディスク状記録媒体30の初期化に用いる装置やファームウェアや初期化ツールのバージョン、ディスク状記録媒体30のプリマスター情報といったものである。

【0106】そして、暗号化部19は、鍵情報生成部f()によって、disk_idとdisk_infoとを用いて記録媒体鍵情報であるdisk_keyを生成する。

【0107】さらに、暗号化部19は、必要に応じて、暗号化/復号化部e()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0108】なお、暗号化部19は、一般に、コントロール領域への各種情報の記録を複数ブロックにわたり行う。ただし、データ記録再生装置10においては、disk_idがディスク状記録媒体30に対して1つであるため、暗号化部19は、ランダムデータをランダムデータ発生部r()により1回のみ発生する。

【0109】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0110】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f()によりdisk_keyを生成する。

【0111】そして、暗号化部19は、記録時におけるディスク状記録媒体30に関する各種情報（記録時情報）であるinfo_bの全部又は一部の情報（ブロック情報）を、図示しないCPUによりblk_infoとして設定され、ユーザ領域のブロック内のIDS領域に記録する。なお、記録時におけるディスク状記録媒体30に関する各種情報とは、例えば、コンテンツの著作権情報やコピー世代管理情報、ユーザデータの記録時に用いる装置やファームウェアのバージョン、アプリケーション側からの制御情報といったものである。

【0112】さらに、暗号化部19は、鍵情報生成部f'()によって、disk_keyとblk_infoとを用いてブロック鍵情報をあるblk_keyを生成する。

【0113】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0114】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0115】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0116】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_infoを取り出し、disk_keyとblk_infoとを用いて鍵情報生成部f'()によりblk_keyを生成する。

【0117】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0118】なお、ユーザ領域のブロックから取り出されたblk_infoは、アプリケーション側に直接出力されることはない。blk_infoは、必要な場合に、必要な情報のみ、例えば図示しないCPUを介して、或いは、専用の信号線を用いて出力され、例えば暗号化されたコンテンツの復号化のために用いられる。

【0119】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0120】データ記録再生装置10は、このように暗号化部19が動作することによって、disk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができます。

【0121】つぎに、データ記録再生装置10における第2の実施の形態について図8を用いて説明する。この第2の実施の形態は、データ記録再生装置10は、disk_idの他にblk_idをも用いてデータを暗号化し、blk_keyを解読されにくくするために各ブロック毎に変えられるようになるものである。すなわち、この第2の実施の形態では、第1の実施の形態として示したように、disk_keyのみでデータを暗号化するのではない。同図には、ユーザ領域及びコントロール領域のそれれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部

19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、パリティは含まれていない。

【0122】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び／又は復号化を行うコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部e()及びユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r(), r'(), 鍵情報生成部f(), f'(), 暗号化／復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0123】このような暗号化部19は、ディスク状記録媒体30の初期化時には、上述した第1の実施の形態として説明したものと同様の動作を行う。すなわち、暗号化部19は、ランダムデータ発生部r()によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体30に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のFS領域に記録する。

【0124】また、暗号化部19は、初期化時におけるディスク状記録媒体30に関する各種情報であるinfo_dの全部又は一部の情報を、図示しないCPUによりdisk_infoとして設定され、コントロール領域のブロック内のIDS領域に記録する。

【0125】そして、暗号化部19は、鍵情報生成部f()によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【0126】さらに、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0127】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0128】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0129】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ

部以外のF S領域に記録する。

【0130】さらに、暗号化部19は、記録時におけるディスク状記録媒体30に関する各種情報を、図示しないCPUによりblk_infoの全部又は一部の情報を、図示しないCPUによりblk_infoとして設定され、ユーザ領域のブロック内のIDS領域に記録する。

【0131】また、暗号化部19は、鍵情報生成部f'()によって、disk_keyとblk_idとblk_infoとを用いてblk_keyを生成する。

【0132】そして、暗号化部19は、必要に応じて、暗号化/復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0133】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0134】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0135】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、disk_keyとblk_idとblk_infoとを用いて鍵情報生成部f'()によりblk_keyを生成する。

【0136】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化/復号化部e'()によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0137】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0138】ディスク状記録媒体30においては、disk_keyが固定であるとともに、blk_infoも一定となることがある。すなわち、blk_infoのもととなるinfo_bは、上述したように、コンテンツの著作権情報やコピー世代管理情報といったコンテンツ単位の情報である場合がある。そのため、例えば動画データ等の多くのブロックに記録されるコンテンツが記録されたブロックに関するinfo_blkは、ブロック間で一定となる。データ記録再生装置10は、このような場合にも効果を奏するものであり、図8に示したように暗号化部19が動作することによって、blk_keyを解読されにくく、各ブロック毎に変えることができることから、disk_id,blk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【0139】つぎに、データ記録再生装置10における

第3の実施の形態について図9を用いて説明する。この第3の実施の形態は、データ記録再生装置10は、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化するものである。すなわち、この第3の実施の形態は、info_d,info_bが不当な第三者に知られることを防止するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるF S、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのF S領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、パリティは含まれていない。

【0140】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び/又は復号化を行うコントロール領域用暗号化及び/又は復号化手段である暗号化/復号化部e()及びユーザ領域用暗号化及び/又は復号化手段である暗号化/復号化部e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r(), r'(), 鍵情報生成部f(), f'(), 暗号化/復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0141】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r()によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体30に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のF S領域に記録する。

【0142】また、暗号化部19は、必要に応じて鍵情報生成部f'()によって、disk_idと、初期化時におけるディスク状記録媒体30に関する各種情報を、info_dの全部又は一部の情報を用いてdisk_keyを生成する。暗号化部19は、生成したdisk_keyをdisk_infoとしてコントロール領域のブロック内のIDS領域に記録する。

【0143】そして、暗号化部19は、必要に応じて、暗号化/復号化部e'()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0144】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0145】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、鍵情報生成部f'()に

よりdisk_infoを取り出してdisk_keyを生成する。

【0146】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ部以外のFS領域に記録する。

【0147】さらに、暗号化部19は、必要に応じて鍵情報生成部f'()によって、disk_keyと、blk_idと、記録時におけるディスク状記録媒体30に関する各種情報であるinfo_bの全部又は一部の情報を用いてblkkeyを生成する。暗号化部19は、生成したblk_keyをblk_infoとしてユーザ領域のブロック内のIDS領域に記録する。

【0148】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0149】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0150】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、鍵情報生成部f()によりdisk_infoを取り出してdisk_keyを生成する。

【0151】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、disk_keyとblk_idとblk_infoとを用いて鍵情報生成部f'()によりblk_keyを生成する。

【0152】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0153】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0154】データ記録再生装置10は、このように暗号化部19が動作することによって、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化することができる。そのため、データ記録再生装置10は、上述したデータ処理部とバッファメモリ16との間の信号をモニタされることによって、disk_info及びblk_infoがそれぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のIDS領域から取り出され、info_d及びinfo_bが不当な第三者に知られることを防止することができることから、disk_id,blk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とするこ

とができる。

【0155】つぎに、データ記録再生装置10における第4の実施の形態について図10を用いて説明する。この第4の実施の形態は、データ記録再生装置10は、第3の実施の形態と同様に、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化するものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、バリティは含まれていない。

【0156】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び／又は復号化を行う第1及び第2のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部g(),e'()及び第1及び第2のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部g'(),e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r(),r'(),鍵情報生成部f(),f'(),暗号化／復号化部g(),g'(),暗号化／復号化部e(),e'()は、それれ、共通化されてもよい。

【0157】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r()によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体30に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のFS領域に記録する。

【0158】また、暗号化部19は、必要に応じて暗号化／復号化部g()によって、disk_idを用いて、初期化時におけるディスク状記録媒体30に関する各種情報を用いてdisk_infoを生成する。暗号化部19は、生成したdisk_infoをコントロール領域のブロック内のIDS領域に記録する。

【0159】さらに、暗号化部19は、鍵情報生成部f()によって、disk_infoをdisk_keyとする。

【0160】そして、暗号化部19は、必要に応じて、暗号化／復号化部e()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0161】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0162】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_infoを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0163】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ部以外のFS領域に記録する。

【0164】さらに、暗号化部19は、必要に応じて暗号化／復号化部g'()によって、disk_keyとblk_idとを用いて、記録時におけるディスク状記録媒体30に関する各種情報であるinfo_bの全部又は一部の情報を暗号化し、blk_infoを生成する。暗号化部19は、生成したblk_infoをユーザ領域のブロック内のIDS領域に記録する。

【0165】また、暗号化部19は、鍵情報生成部f'()によって、blk_infoをblk_keyとする。

【0166】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0167】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0168】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_infoを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0169】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_infoを取り出し、disk_keyとblk_infoとを用いて鍵情報生成部f'()によりblk_keyを生成する。

【0170】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0171】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0172】データ記録再生装置10は、このように暗号化部19が動作することによって、disk_info,blk_infoもそれぞれdisk_id,blk_idを用いて暗号化することができる。そのため、データ記録再生装置10は、上述したデータ処理部とバッファメモリ16との間の信号をモニタされることによって、disk_info及びblk_infoがそ

れぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のIDS領域から取り出され、info_d及びinfo_bが不当な第三者に知られることを防止することができることから、disk_id,blk_idに基づいて生成されたdisk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【0173】つぎに、データ記録再生装置10における第5の実施の形態について図11を用いて説明する。この第5の実施の形態では、データ記録再生装置10は、仮にblk_infoが不当な第三者に知られてもuser_dataが知られることがないものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、バリティは含まれていない。

【0174】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()と、鍵情報を分割するコントロール領域用鍵情報分割手段である鍵情報分割部d()及びユーザ領域用鍵情報分割手段である鍵情報分割部d'()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び／又は復号化を行う第1及び第2のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部g(), e()及び第1及び第2のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部g'(), e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r(), r'(), 鍵情報分割部d(), d'(), 鍵情報生成部f(), f'(), 暗号化／復号化部g(), g'(), 暗号化／復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0175】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r()によりランダムデータを発生させ、このランダムデータを、上述したように、ディスク状記録媒体30に固有のdisk_idとし、コントロール領域のブロック内のデータ部以外のFS領域に記録する。

【0176】また、暗号化部19は、必要に応じて鍵情報分割部d()によって、ランダムデータ発生部r()により発生されたランダムデータを分割する。

【0177】そして、暗号化部19は、暗号化／復号化

部g()によって、鍵情報分割部d()により分割された一方のランダムデータを用いて、初期化時におけるディスク状記録媒体30に関する各種情報であるinfo_dの全部又は一部の情報を暗号化し、disk_infoを生成する。暗号化部19は、生成したdisk_infoをコントロール領域のブロック内のIDS領域に記録する。

【0178】さらに、暗号化部19は、鍵情報生成部f()によって、鍵情報分割部d()により分割された他方のランダムデータと、disk_infoとを用いてdisk_keyを生成する。

【0179】なお、暗号化部19においては、必ずしも鍵情報分割部d()によりランダムデータ発生部r()により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部r()によって、互いに異なる2つのランダムデータを発生し、これら2つのランダムデータをblk_idとし、一方のランダムデータを用いてdisk_infoを生成するとともに、他方のランダムデータを用いてdisk_keyを生成するようにしてもよい。

【0180】そして、暗号化部19は、必要に応じて、暗号化／復号化部e()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0181】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0182】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、blk_idとdisk_infoとを取り出して鍵情報生成部f()によりdisk_keyを生成する。

【0183】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30のブロックに固有のblk_idとし、ユーザ領域のブロック内のデータ部以外のFS領域に記録する。

【0184】また、暗号化部19は、必要に応じて鍵情報分割部d'()によって、ランダムデータ発生部r'()により発生されたランダムデータを分割する。

【0185】さらに、暗号化部19は、暗号化／復号化部g'()によって、鍵情報分割部d'()により分割された一方のランダムデータを用いて、記録時におけるディスク状記録媒体30に関する各種情報であるinfo_bの全部又は一部の情報を暗号化し、blk_infoを生成する。暗号化部19は、生成したblk_infoをユーザ領域のブロック内のIDS領域に記録する。

【0186】さらに、暗号化部19は、鍵情報生成部f'()によって、鍵情報分割部d'()により分割された他方のランダムデータと、blk_infoと、disk_keyとを用いてblk_keyを生成する。

【0187】なお、暗号化部19においては、必ずしも鍵情報分割部d'()によりランダムデータ発生部r'

()により発生されたランダムデータを分割する必要はなく、ランダムデータ発生部r'()によって、互いに異なる2つのランダムデータを発生し、これら2つのランダムデータをblk_idとし、一方のランダムデータを用いてblk_infoを生成するとともに、他方のランダムデータを用いてblk_keyを生成するようにしてもよい。

【0188】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0189】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0190】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、blk_idとdisk_idとdisk_infoとを取り出して鍵情報生成部f()によりdisk_keyを生成する。

【0191】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、blk_idとblk_infoとdisk_keyとを用いて鍵情報生成部f'()によりblk_keyを生成する。

【0192】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0193】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0194】データ記録再生装置10は、このように暗号化部19が動作することによって、仮にblk_infoが不当な第三者に知られてもuser_dataが知られることがない。そのため、データ記録再生装置10は、上述したデータ処理部とバッファメモリ16との間の信号をモニタされることによって、disk_info及びblk_infoがそれぞれ不当な第三者によりコントロール領域及びユーザ領域のブロック内のIDS領域から取り出されてdisk_key及びblk_keyが不当な第三者に知られた場合にも効果を奏するものであり、disk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができます。

【0195】つぎに、データ記録再生装置10における第6の実施の形態について図12を用いて説明する。この第6の実施の形態では、データ記録再生装置10は、コントロール領域内の各ブロックにおいて互いに異なるdisk_idを用いるものである。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成され

る1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、パリティは含まれていない。

【0196】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r'()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()'と、鍵情報を分割するコントロール領域用鍵情報分割手段である鍵情報分割部d'()及びユーザ領域用鍵情報分割手段である鍵情報分割部d'()'と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f'()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()'と、暗号化及び／又は復号化を行う第1、第2及び第3のコントロール領域用暗号化及び／又は復号化手段である暗号化／復号化部b'(), g'(), e'()及び第1、第2及び第3のユーザ領域用暗号化及び／又は復号化手段である暗号化／復号化部b'(), g'(), e'()とを有する。なお、コントロール領域及びユーザ領域のそれそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r'(), r'()'、鍵情報分割部d'(), d'()'、鍵情報生成部f'(), f'()'、暗号化／復号化部b'(), b'()'、暗号化／復号化部g'(), g'()'、暗号化／復号化部e'(), e'()'は、それぞれ、共通化されてもよい。

【0197】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、図示しないCPUにより設定された物理ブロック番号(blk_no)を用いて、暗号化／復号化部b'()により暗号化し、各ブロック毎に固有のdisk_idを生成する。暗号化部19は、生成したdisk_idをコントロール領域のブロック内のデータ部以外のFS領域に記録する。

【0198】また、暗号化部19は、必要に応じて鍵情報分割部d'()によって、ランダムデータ発生部r'()により発生されたランダムデータを分割する。

【0199】そして、暗号化部19は、暗号化／復号化部g'()によって、鍵情報分割部d'()により分割された一方のランダムデータを用いて、初期化時におけるディスク状記録媒体30に関する各種情報であるinfo_dの全部又は一部の情報を暗号化し、disk_infoを生成する。暗号化部19は、生成したdisk_infoをコントロール領域のブロック内のIDS領域に記録する。

【0200】さらに、暗号化部19は、鍵情報生成部f'()によって、鍵情報分割部d'()により分割された他方のランダムデータと、disk_infoとを用いてdisk_key

を生成する。

【0201】なお、暗号化部19においては、必ずしも鍵情報分割部d'()によりランダムデータ発生部r'()により発生されたランダムデータを分割する必要はない、ランダムデータ発生部r'()によって、互いに異なる2つのランダムデータを発生し、これら2つのランダムデータをblk_idとし、一方のランダムデータを用いてdisk_infoを生成するとともに、他方のランダムデータを用いてdisk_keyを生成するようにしてもよい。

【0202】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0203】なお、暗号化部19は、info_dとblk_noが含まれていない場合には、disk_infoやcont_dataをblk_idを用いて暗号化するようにしてもよい。

【0204】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0205】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f'()によりdisk_keyを生成する。

【0206】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、図示しないCPUにより設定されたblk_noを用いて、暗号化／復号化部b'()により暗号化し、各ブロック毎に固有のblk_idを生成する。暗号化部19は、生成したblk_idをユーザ領域のブロック内のデータ部以外のFS領域に記録する。

【0207】また、暗号化部19は、必要に応じて鍵情報分割部d'()によって、ランダムデータ発生部r'()により発生されたランダムデータを分割する。

【0208】さらに、暗号化部19は、暗号化／復号化部g'()によって、鍵情報分割部d'()により分割された一方のランダムデータを用いて、記録時におけるディスク状記録媒体30に関する各種情報であるinfo_bの全部又は一部の情報を暗号化し、blk_infoを生成する。暗号化部19は、生成したblk_infoをユーザ領域のブロック内のIDS領域に記録する。

【0209】さらに、暗号化部19は、鍵情報生成部f'()によって、鍵情報分割部d'()により分割された他方のランダムデータと、blk_infoと、disk_keyとを用いてblk_keyを生成する。

【0210】なお、暗号化部19においては、必ずしも鍵情報分割部d'()によりランダムデータ発生部r'()により発生されたランダムデータを分割する必要はない、ランダムデータ発生部r'()によって、互いに異なる2つのランダムデータを発生し、これら2つのランダムデータをblk_idとし、一方のランダムデータを用

いてblk_infoを生成するとともに、他方のランダムデータを用いてblk_keyを生成するようにしてもよい。

【0211】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'（）によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0212】なお、暗号化部19は、各部の共通化を図り、blk_id,blk_info,blk_dataをblk_noを用いて暗号化するようにしてもよい。

【0213】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。

【0214】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f（）によりdisk_keyを生成する。

【0215】そして、暗号化部19は、ユーザ領域のブロックを再生し、再生されたユーザ領域のブロックからblk_idとblk_infoとを取り出し、blk_idとblk_infoとdisk_keyとを用いて鍵情報生成部f'（）によりblk_keyを生成する。

【0216】また、暗号化部19は、再生されたユーザ領域のブロックからのblk_dataを、必要に応じて、暗号化／復号化部e'（）によりblk_keyを用いて復号化し、user_dataとして外部のアプリケーション側へと出力する。

【0217】暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、このように動作する。

【0218】ディスク状記録媒体30におけるコントロール領域には、一般に、制御情報が複数ブロックにわたって記録されるが、disk_keyは同一である必要がある。そのため、blk_idやblk_infoが全てのブロック間で同一となり、disk_keyが解読されやすいおそれがある。データ記録再生装置10は、このような場合にも効果を奏ずるものであり、図12に示したように暗号化部19が動作することによって、コントロール領域内の各ブロックにおいて互いに異なるdisk_idを用いることから、データの解読やディスクコピーを困難とすることができます。

【0219】ところで、多数のブロックに記録されるべき暗号化される前のuser_dataと多数のブロックに記録されている暗号化された後のblk_dataとが不当な第三者に知られると、blk_keyが知られるおそれがある。blk_keyが第三者に知られると、user_dataの解読やディスクコピーが可能となる。

【0220】そこで、以上のようなデータ記録再生装置10は、暗号化されたデータを復号化しないで外部のアプリケーション側又は図示しないCPUに出力することを禁止することもできる。この場合、データ記録再生装

置10は、ファームウェアで対処することもできるが、改変される危険性を考慮して、ハードウェアでデータの出力を禁止する。データ記録再生装置10は、暗号化部19によって、再生されたdataやinfoが暗号化されているか否かを判別し、入出力部20への出力を制御する。

【0221】具体的には、データ記録再生装置10は、暗号化部19による判別の結果、control_data又はuser_dataの再生時に、再生されたブロックからのdisk_id若しくはblk_id又はcont_data若しくはblk_data又はdisk_info若しくはblk_infoが暗号化されていることを示していた場合には、暗号化部19によって、復号化して出力すべき旨の正しいコマンドを受けた場合にのみ、cont_data若しくはblk_dataを復号化して出力し、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力しない。

【0222】一方、データ記録再生装置10は、暗号化部19による判別の結果、再生されたブロックからのdisk_id若しくはblk_id又はcont_data若しくはblk_data又はdisk_info若しくはblk_infoが暗号化されていないことを示していた場合には、暗号化部19によって、復号化して出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力せず、復号化しないでそのまま出力すべき旨のコマンドを受けた場合には、cont_data若しくはblk_dataを復号化して出力する。

【0223】さらに、データ記録再生装置10は、図示しないインターフェースを介してバッファメモリ16に保持されている各種情報が図示しないCPUに出力されるとともに、図示しないインターフェースを介して図示しないCPUからの各種情報がバッファメモリ16に供給される。そのため、データ記録再生装置10は、バッファメモリ16に保持されているdisk_infoやblk_infoを図示しないCPUに出力することが可能であるが、cont_data若しくはblk_dataと同様に、暗号化部19による判別に応じて、disk_infoやblk_infoの出力を制御する。

【0224】このようにすることによって、データ記録再生装置10は、user_dataの解読やディスクコピーに対するセキュリティを向上させることができる。

【0225】さらに、データ記録再生装置10においては、上述したように、暗号化部19をデータ処理部内に構成することによって、先に図1及び図2に示したフォーマットのディスク状記録媒体30を適用することができ、上述した第1乃至第6の実施の形態として示した方法を用いることができる。これらの場合において、データ処理部とバッファメモリ16との間の信号をモニタされる危険性があることを述べたが、この危険性に対処するために、データ記録再生装置10は、バッファメモリ16をデータ処理部内にチップ化して構成することもで

きる。

【0226】このようにすることによって、データ記録再生装置10は、データ処理部とバッファメモリ16との間の信号をモニタされる危険性がなくなり、安全性を大幅に向上させることができる。

【0227】さらに、データ記録再生装置10は、必要に応じて、信号検出部14もデータ処理部内にチップ化して構成することによって、変調前のデータを不当な第三者に知られることがなくなり、より安全なシステムを構築することができる。

【0228】なお、バッファメモリ16をデータ処理部内にチップ化して構成する場合、データ記録再生装置10においては、レジスタ21を調停部17を通してバッファメモリ16と共に通化してもよい。

【0229】このように、バッファメモリ16をデータ処理部内にチップ化して構成することによって、ディスク状記録媒体30におけるブロック内のデータが外部に漏洩する危険性が小さい場合には、データ記録再生装置10は、disk_idやblk_idをコントロール領域又はユーザ領域のブロック内のデータ部以外のFS領域に記録する必要はなく、コントロール領域又はユーザ領域のブロック内のIDS領域に記録するようにしてもよい。この場合、データ記録再生装置10における暗号化部19の具体的な動作は、図13又は図14に示すようになる。

【0230】まず、第7の実施の形態として図13に示すデータ記録再生装置10について説明する。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、バリティは含まれていない。

【0231】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び/又は復号化を行うコントロール領域用暗号化及び/又は復号化手段である暗号化/復号化部e()及びユーザ領域用暗号化及び/又は復号化手段である暗号化/復号化部e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、鍵情報生成部f(), f'(), 暗号化/復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0232】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部r()によりランダムデータを発生させ、このランダム

データを、ディスク状記録媒体30に固有のdisk_idとともに、初期化時におけるディスク状記録媒体30に関する各種情報をあるinfo_dの全部又は一部の情報を、図示しないCPUによりdisk_infoとして設定され、これらのdisk_id及びdisk_infoをコントロール領域のブロック内のIDS領域に記録する。

【0233】また、暗号化部19は、鍵情報生成部f()によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【0234】さらに、暗号化部19は、必要に応じて、暗号化/復号化部e()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0235】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。なお、暗号化部19は、disk_id及びdisk_infoをコントロール領域のブロック内のIDS領域に記録するのではなく、cont_dataとともにコントロール領域のブロック内のUDS領域に記録するようにしてよい。

【0236】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時及びディスク状記録媒体30に記録されているユーザデータの再生時には、上述した第1の実施の形態と同様に動作する。

【0237】さらに、第8の実施の形態として図14に示すデータ記録再生装置10について説明する。同図には、ユーザ領域及びコントロール領域のそれぞれにおけるFS、720バイトのIDS及び64KバイトのUDSにより構成される1ブロックのデータを示すとともに、これらのFS領域、IDS領域及びUDS領域に対して暗号化部19における各部により入出力される各種情報を示している。なお、1ブロックのデータには、バリティは含まれていない。

【0238】データ記録再生装置10において、暗号化部19は、同図に示すように、ランダムデータを発生するコントロール領域用ランダムデータ発生手段であるランダムデータ発生部r()及びユーザ領域用ランダムデータ発生手段であるランダムデータ発生部r'()と、鍵情報を生成するコントロール領域用鍵情報生成手段である鍵情報生成部f()及びユーザ領域用鍵情報生成手段である鍵情報生成部f'()と、暗号化及び/又は復号化を行うコントロール領域用暗号化及び/又は復号化手段である暗号化/復号化部e()及びユーザ領域用暗号化及び/又は復号化手段である暗号化/復号化部e'()とを有する。なお、コントロール領域及びユーザ領域のそれぞれにおける各部は、共通化されてもよく、例えば、ランダムデータ発生部r(), r'(), 鍵情報生成部f(), f'(), 暗号化/復号化部e(), e'()は、それぞれ、共通化されてもよい。

【0239】このような暗号化部19は、ディスク状記録媒体30の初期化時には、ランダムデータ発生部

r()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30に固有のdisk_idとともに、初期化時におけるディスク状記録媒体30に関する各種情報であるinfo_dの全部又は一部の情報を、図示しないCPUによりdisk_infoとして設定され、これらのdisk_id及びdisk_infoをコントロール領域のブロック内のIDS領域に記録する。

【0240】また、暗号化部19は、鍵情報生成部f()によって、disk_idとdisk_infoとを用いてdisk_keyを生成する。

【0241】さらに、暗号化部19は、必要に応じて、暗号化／復号化部e()によりdisk_keyを用いてcontrol_dataを暗号化し、cont_dataとしてコントロール領域のブロック内のUDS領域に記録する。

【0242】暗号化部19は、ディスク状記録媒体30の初期化時には、このように動作する。

【0243】また、暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、予めコントロール領域のブロックを再生し、disk_idとdisk_infoとを取り出して鍵情報生成部f()によりdisk_keyを生成する。

【0244】そして、暗号化部19は、ランダムデータ発生部r'()によりランダムデータを発生させ、このランダムデータを、ディスク状記録媒体30のブロックに固有のblk_idとともに、記録時におけるディスク状記録媒体30に関する各種情報であるinfo_bの全部又は一部の情報を、図示しないCPUによりblk_infoとして設定され、これらのblk_id及びblk_infoをユーザ領域のブロック内のIDS領域に記録する。

【0245】また、暗号化部19は、鍵情報生成部f'()によって、disk_keyとblk_idとblk_infoとを用いてblk_keyを生成する。

【0246】そして、暗号化部19は、必要に応じて、暗号化／復号化部e'()によりblk_keyを用いてuser_dataを暗号化し、blk_dataとしてユーザ領域のブロック内のUDS領域に記録する。

【0247】暗号化部19は、ディスク状記録媒体30に対するユーザデータの記録時には、このように動作する。なお、暗号化部19は、blk_id及びblk_infoをユーザ領域のブロック内のIDS領域に記録するのではなく、blk_dataとともにユーザ領域のブロック内のUDS領域に記録するようにしてよい。

【0248】さらに、暗号化部19は、ディスク状記録媒体30に記録されているユーザデータの再生時には、上述した第2の実施の形態と同様に動作する。

【0249】このように、データ記録再生装置10は、バッファメモリ16をデータ処理部内にチップ化して構成することによって、disk_idやblk_idをコントロール領域又はユーザ領域のブロック内のIDS領域に記録することができ、図13又は図14に示したように暗号化

部19が動作することによって、disk_key,blk_keyを用いてデータを暗号化することができ、データの解読やディスクコピーを困難とすることができる。

【0250】なお、ここでは、第7及び第8の実施の形態として、バッファメモリ16をデータ処理部内にチップ化して構成することにより上述した第1及び第2の実施の形態を変化させたデータ記録再生装置10について説明したが、上述した第3乃至第6の実施の形態についても同様に適用できることはいうまでもない。

【0251】また、データ記録再生装置10においては、定められた暗号フォーマットに対して、一意に構成が定まるのは勿論である。例えば、第8の実施の形態として示した方法を用いる場合には、データ記録再生装置10は、バッファメモリ16と暗号化部19とがデータ処理部内に構成されている必要がある。

【0252】さらに、データ記録再生装置10は、暗号化部19の内部に図示しないメモリを設け、又は、データ処理部内にバッファメモリ16を構成し、例えば、disk_infoやblk_infoとして、当該データ記録再生装置10を製造するメーカーの情報(maker_info)や当該データ記録再生装置10を示す情報(device_info)をディスク状記録媒体30に記録すべく、各メーカー毎、データ処理部を構成する各IC(Integrated Circuit)の種類又は世代毎に固有の情報を予めメモリ又はバッファメモリ16に保持させておくこともできる。これらのmaker_infoやdevice_info等の情報は、例えば、商品化されるデータ記録再生装置におけるデータ処理部によっては出力されないようにしたり、ライセンスを管理するベンダが有するデータ記録再生装置におけるデータ処理部によってのみ出力可能とされる。

【0253】このようにすることによって、不当な第三者により違法なデータの解読やディスクコピーがされた場合にも、ディスク状記録媒体30の初期化やデータの記録がどのような装置や環境により行われたかを示す情報等を得ることができる。

【0254】以上説明してきたように、本発明の実施の形態として示すデータ記録再生装置10は、暗号化された後のデータやデータを暗号化するための各種情報を第三者に知られることを防止することができ、データや鍵情報の解読を困難とすることができます。

【0255】また、データ記録再生装置10は、暗号化及び復号化の方法が公になった場合又は仮にディスク状記録媒体30に固有の鍵情報が第三者に知られた場合でも、ブロックに固有の鍵情報を用いてデータをブロック毎に暗号化することによって、データの解読を困難とすることができる。

【0256】データ記録再生装置10は、データや鍵情報の解読を困難とすることによって、データの違法なコピーやディスクコピーを防止することができる。さらに、仮に不当な第三者によりデータの違法なコピーやデ

ィスクコピーがされた場合であっても、どのような装置や環境によりディスク状記録媒体30の初期化やデータの記録が行われたかを示す情報を得ることができ、データの違法なコピーやディスクコピーの防止の一助となる。

【0257】なお、本発明は、上述した実施の形態に限定されるものではなく、例えば、いわゆる光ディスクのようなディスク状記録媒体に対するデータの記録及び／又は再生を行うものとして説明したが、データをストレージする記録媒体であれば光ディスク以外の記録媒体にも応用できるものである。

【0258】また、上述した実施の形態では、図3に示したデータ記録再生装置10について説明したが、上述したように、「アプリケーション側との入出力方向」と「暗号化方向」と「ECC方向」とが同一であれば、図15に示すデータ記録再生装置40であってもよい。

【0259】このデータ記録再生装置40は、上述したスピンドルモータ11、光学ピックアップ12、レザードライバ13、信号検出部14、変復調部15及びバッファメモリ16の他に、バッファメモリ16と、変復調部15、後述するECC部48との間で行われるデータの入出力を調停する調停部47と、データに対する誤り訂正及び／又は誤り検出を行うECC部48と、後述する入出力部50から供給される記録すべきデータを暗号化するとともに、ECC部48から供給される再生すべきデータを復号化する暗号化部49と、外部とのデータの入出力を行うためのインターフェースである入出力部50と、データに対する暗号化及び復号化に必要となる各種情報を保持するレジスタ51、52とを備える。

【0260】すなわち、データ記録再生装置40は、データ記録再生装置10と比較して、調停部47によりデータの入出力を調停する必要がある各部が少ない。そのため、データ記録再生装置40は、調停部47によるデータの入出力の調停を容易に行うことができる。なお、データ記録再生装置40によるディスク状記録媒体30の初期化、ディスク状記録媒体30に対するユーザデータの記録及びディスク状記録媒体30に記録されているデータの再生動作は、上述したデータ記録再生装置10における第1乃至第8の実施の形態と同様であるため、ここでは説明を省略する。

【0261】このように、本発明は、その趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【0262】

【発明の効果】以上詳細に説明したように、本発明にかかるデータ記録再生方法は、ディスク状記録媒体に対するプロック単位でのデータの記録及び／又は再生を行うデータ記録再生方法であって、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報とディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化する。

定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化する。

【0263】したがって、本発明にかかるデータ記録再生方法は、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化することによって、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とすることができる。

【0264】また、本発明にかかるデータ記録再生装置は、ディスク状記録媒体に対するプロック単位でのデータの記録及び／又は再生を行うデータ記録再生装置であって、ディスク状記録媒体に対して記録すべきデータを暗号化するとともに、ディスク状記録媒体に記録されている再生すべきデータを復号化する暗号化手段を少なくとも有してデータ処理を行うデータ処理手段を備え、暗号化手段は、ディスク状記録媒体の初期化時に、ディスク状記録媒体に固有の記録媒体識別情報をディスク状記録媒体のコントロール領域における所定領域に記録し、ディスク状記録媒体に対するユーザデータの記録時に、記録媒体識別情報を用いてユーザデータを暗号化する。

【0265】したがって、本発明にかかるデータ記録再生装置は、暗号化手段によって、ディスク状記録媒体のコントロール領域における所定領域に記録されているディスク状記録媒体に固有の記録媒体識別情報を用いてユーザデータを暗号化することによって、ディスク状記録媒体に記録されているデータの解読やディスクコピーを困難とすることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態として示すデータ記録再生装置に適用されるディスク状記録媒体におけるフォーマットを説明する図であって、1プロック分を示す図である。

【図2】ディスク状記録媒体におけるフォーマットを説明する図であって、ディスク状記録媒体上に並べられるパリティ以外のデータを示す図である。

【図3】同データ記録再生装置の構成を説明するブロック図である。

【図4】同データ記録再生装置がディスク状記録媒体を初期化する際の一連の工程を説明するフローチャートである。

【図5】同データ記録再生装置がディスク状記録媒体に対してユーザデータを記録する際の一連の工程を説明するフローチャートである。

【図6】同データ記録再生装置がディスク状記録媒体に記録されているユーザデータを再生する際の一連の工程を説明するフローチャートである。

【図7】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第1の実施の形態

として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 8】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第2の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 9】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第3の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 10】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第4の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 11】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第5の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 12】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第6の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 13】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第7の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

* 作内容を説明する図である。

【図 14】同データ記録再生装置における暗号化部の動作内容を説明する図であって、本発明の第8の実施の形態として示すデータ記録再生装置における暗号化部の動作内容を説明する図である。

【図 15】同データ記録再生装置の他の構成を説明するブロック図である。

【図 16】DVDのフォーマットを説明する図であって、1 ブロック分を示す図である。

10 【図 17】DVDのフォーマットを説明する図であって、ディスク状記録媒体上に並べられるパリティ以外のデータを示す図である。

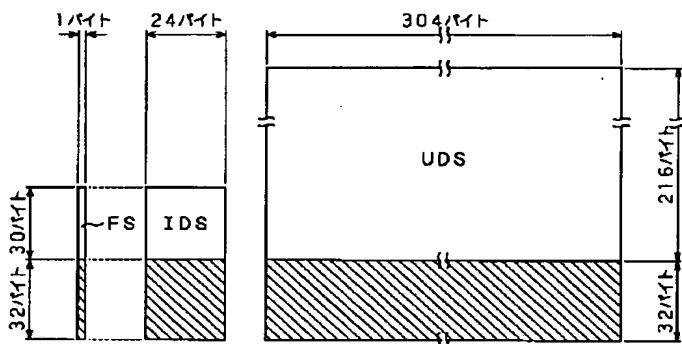
【図 18】従来のデータ記録再生装置の構成を説明するブロック図である。

【符号の説明】

10 データ記録再生装置、 11 スピンドルモーター、 12 光学ピックアップ、 13 レーザドライバ、 14 信号検出部、 15 变復調部、 16 バッファメモリ、 17 調停部、 18 ECC部、

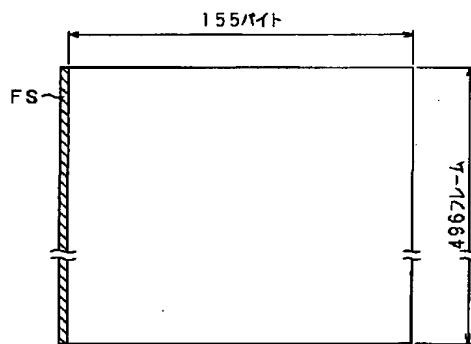
20 19 暗号化部、 20 入出力部、 21, 22 レジスタ、 30 ディスク状記録媒体、 r () , r' () ランダムデータ発生部、 d () , d' () 鍵情報分割部、 f () , f' () 鍵情報生成部、 b () , b' () , g () , g' () , e () , e' () 暗号化／復号化部

【図 1】



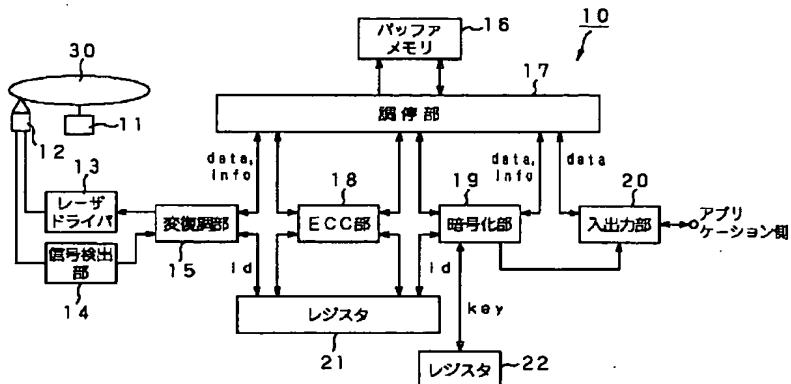
ディスク状記録媒体におけるフォーマットの説明図

【図 2】

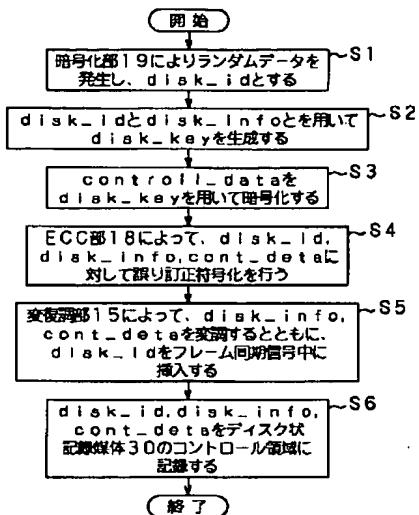


ディスク状記録媒体におけるフォーマットの説明図

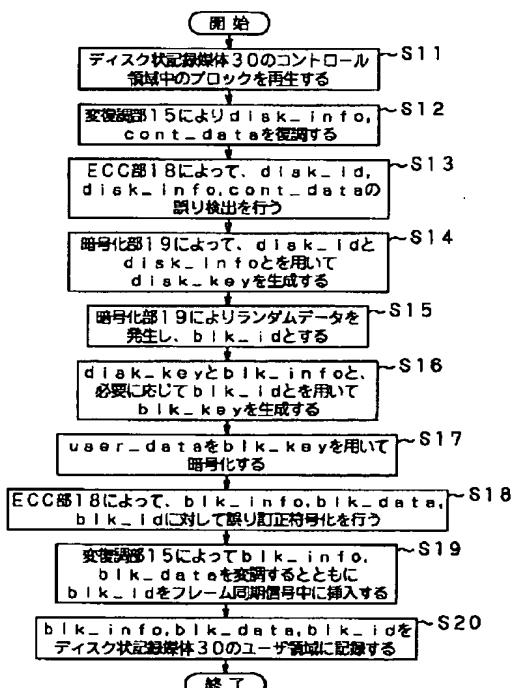
【図3】



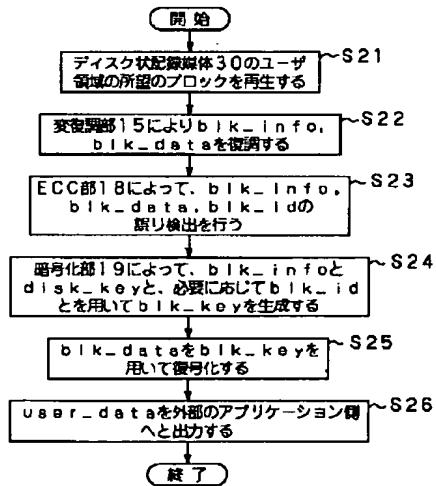
【図4】



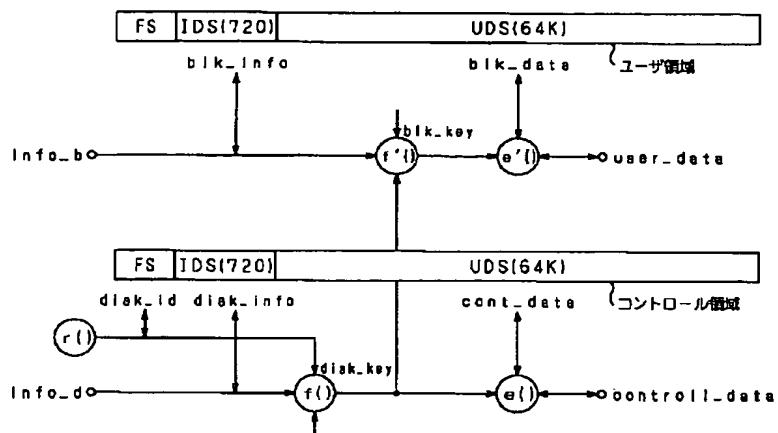
【図5】



【図6】

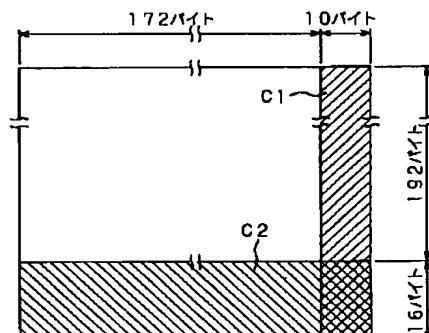


【図7】



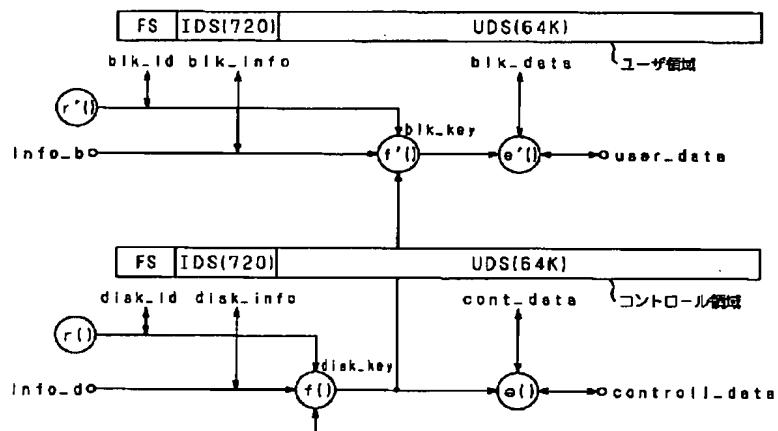
暗号化部の動作内容の説明図

【図16】



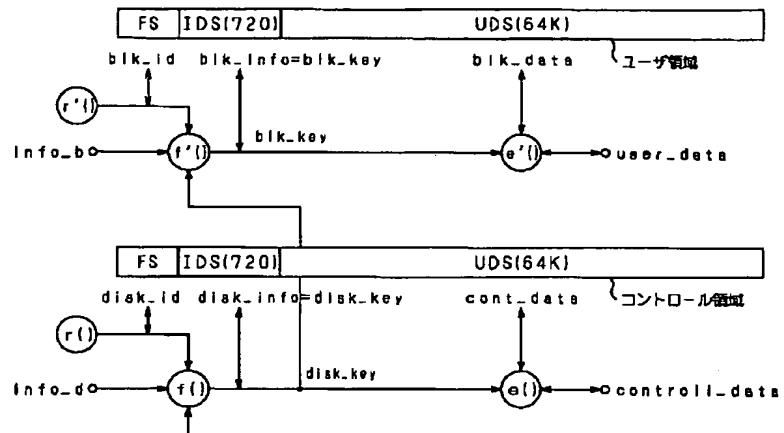
DVDフォーマットの説明図

【図8】



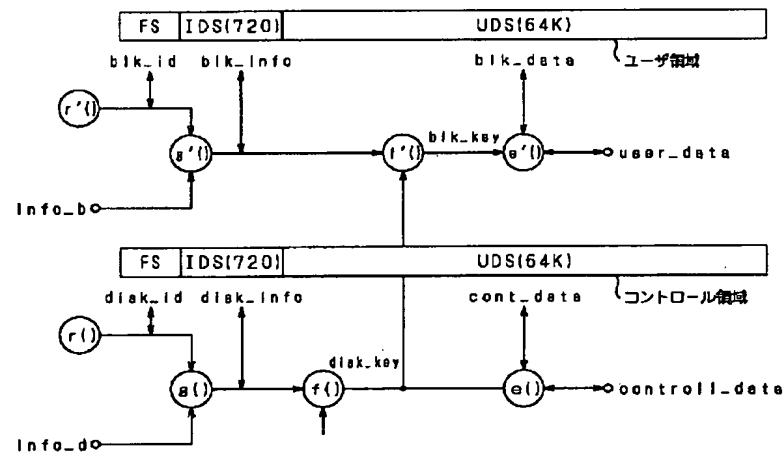
暗号化部の動作内容の説明図

【図9】



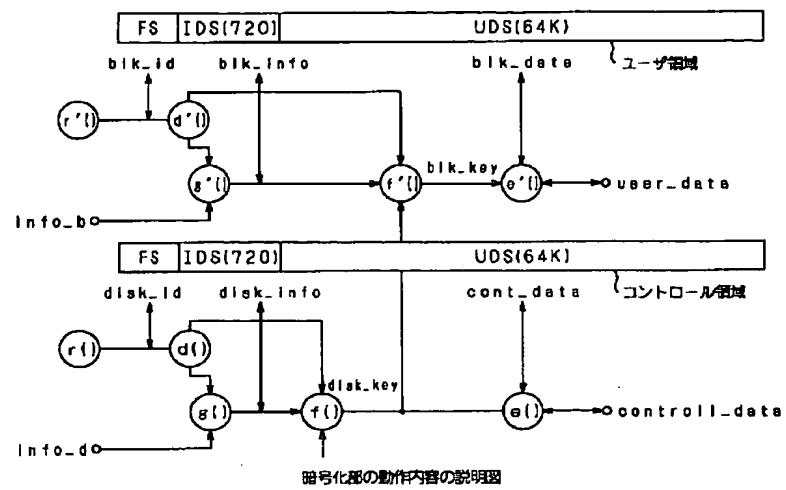
暗号化部の動作内容の説明図

【図10】

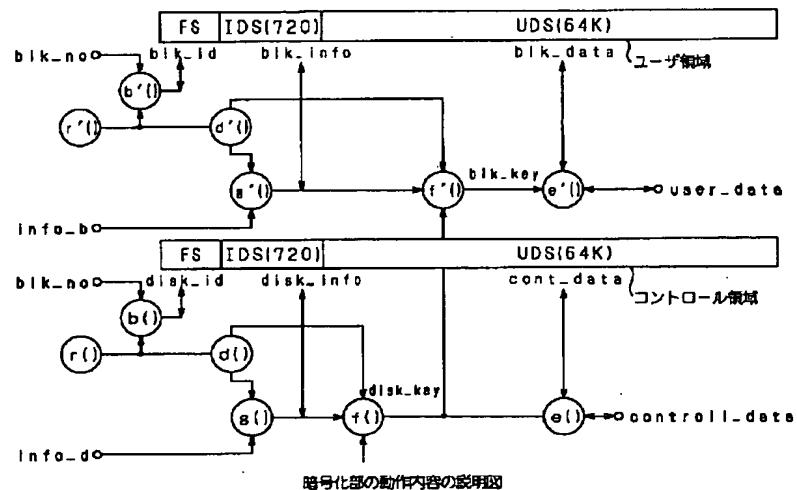


暗号化部の動作内容の説明図

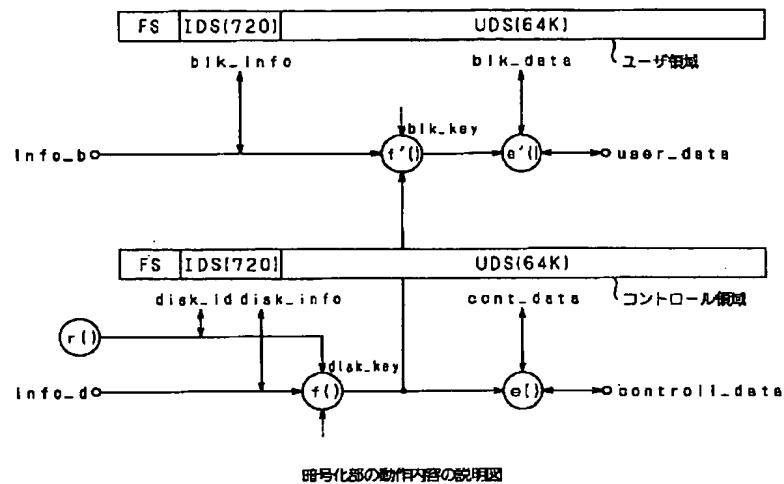
【図11】



【図12】

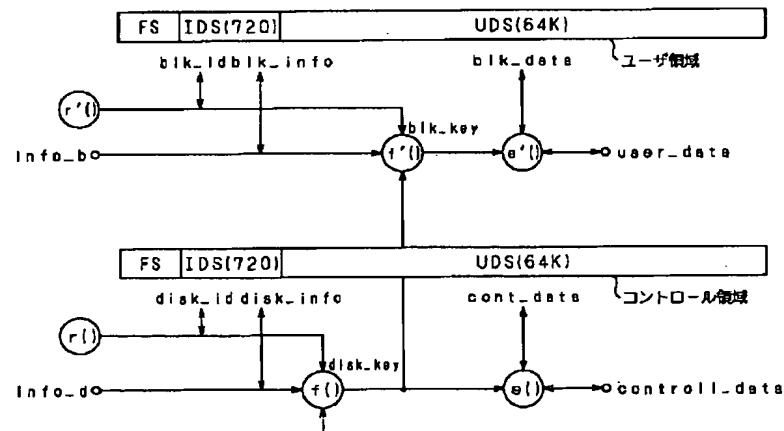


【図13】



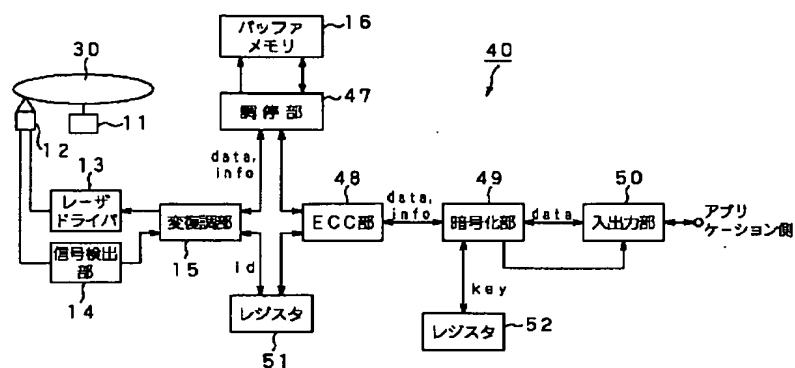
暗号化部の動作内容の説明図

【図14】



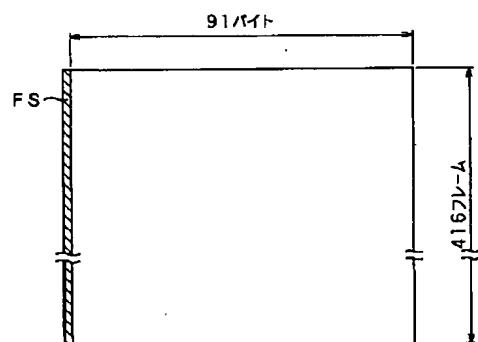
暗号化部の動作内容の説明図

【図15】



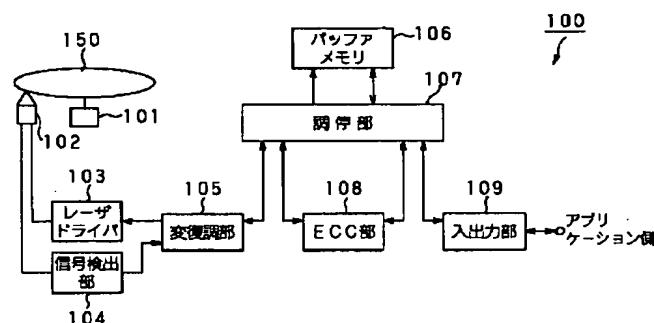
データ記録再生装置の構成ブロック図

【図17】



DVDフォーマットの説明図

【図18】



従来のデータ記録再生装置の構成ブロック図